VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA PRÁVA

Elektronické bankovnictví a možnosti jeho zneužívání

Electronic Banking and the Possibility of its Abuse

Student: Bc. Lucie Stušová
Vedoucí diplomové práce: JUDr. Bohuslav Halfar

Ostrava 2011

VŠB-Technická univerzita Ostrava
Ekonomická fakulta
Katedra Práva

Zadání diplomové práce

Student: **Bc. Lucie Stušová**

Studijní program: N6208 Ekonomika a management

Studijní obor: 6208T011Ekonomika a právo v podnikání

Téma: Elektronické bankovnictví a možnosti jeho zneužívání

Electronic Banking and the Possibility of its Abuse

Zásady pro vypracování

1. Úvod
2. Pojem a historický vývoj elektronického bankovnictví
3. Možnosti zneužití elektronického bankovnictví
4. Prostředky k minimalizaci zneužití elektronického bankovnictví
5. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků bakalářské práce
Přílohy

Seznam doporučené odborné literatury:

JUŘÍK, P. *Platební karty – velká encyklopedie 1870 -2006*. 1 vydání. Praha: Grada Publishing, 2006. 296s. ISBN 80-247-1381-0.
MÁČE, M. *Platební styk – klasický a elektronický*. 1 vydání. Praha: Grada Publishing, 2006. 220s. ISBN 80-247-1725-5.
PŘÁDKA, M.; KALA, J. *Elektronické bankovnictví*. 1 vydání. Praha: Computer Press, 2000. 166s. ISBN 80-7226-328-5.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **JUDr. Bohuslav Halfar**

Datum zadání: 26. 11. 2010

Datum odevzdání: 29. 4. 2011

JUDr. Bohuslav Halfar
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

„Místopřísežně prohlašuji, že jsem celou diplomovou práci, včetně všech příloh, vypracovala samostatně a uvedla jsem veškerou použitou literaturu a další prameny.“

V Ostravě dne 29. dubna 2011 Bc. Lucie Stušová

Ráda bych poděkovala panu JUDr. Bohuslavu Halfarovi za zájem, připomínky a čas, který věnoval mé diplomové práci.

Obsah

1 Úvod

Jako téma této diplomové práce jsem si zvolila téma Elektronické bankovnictví a možnosti jeho zneužívání. Práce se zaměřuje na dvě nejrozšířenější oblasti elektronického neboli přímého bankovnictví, a to platební karty a internetové bankovnictví.

Ještě před několika lety, kdy se v naší zemi začal objevovat první počítače a mobilní telefony, a s tím spojené pojmy jako internetbanking, homebanking či GSM bankovnictví, byli lidé nedůvěřiví, a tvrdili, že se jich to netýká, že takové věci nikdy nebudou potřebovat. V dnešní době se tyto pojmy stali běžnou součástí každodenního života mnoha z nás a tudíž si asi nikdo nebo jen málokdo dokáže představit život bez těchto prostředku komunikace. Třeba si ani někteří z nás neuvědomují, jak moc nám tyto vymoženosti usnadňují život. Před pár lety lidé museli vystát dlouhé fronty v bance či na poště, nebo spěchali z práce, aby ještě stihli jejich otevírací dobu. Dnes je to díky těmto prostředkům přímého bankovnictví daleko jednodušší. Hodně lidí díky přímého bankovnictví ušetří spoustu času. Je daleko pohodlnější si sednout doma k počítači, otevřít internetový prohlížeč a přihlásit se k internetovému bankovnictví své banky. Zde jen člověk udělá pár kliků myší a má vše vyřízeno. Nemusí stát dlouhé fronty v bance a tím pádem si tím ušetří spoustu času a někdy i nervy. Stejné je to i u platebních karet. Pro některé z nás je lepší mít u sebe platební kartu než hotovost. Při platbě v obchodě či v restauraci vytáhnou platební kartu, během pár sekund zadají PIN kód a platba se odečte přímo z účtu. Nemusí se tak zbytečně omezovat hotovostí, kterou mají v té době u sebe.

Také s příchodem internetu lidé častěji využívají nákup z pohodlí domova pomocí e-shopů a dávají mu přednost před kamennými obchody. Někteří k tomu využívají možnost placení prostřednictvím bezhotovostních platebních prostředků.

Ale s nástupem nových technologií přicházejí také možnosti jeho zneužití. Není platebního prostředku, který by se lidé nesnažili nějaký způsobem zneužít. Jedná se buď o běžné způsoby, kdy dojde ke ztrátě platební karty či jejímu odcizení a následnému zneužití. V některých případech se na tom mohou podílet také i osoby blízké aniž by o tom majitel platební karty věděl. Ale častěji se začínají vyskytovat daleko promyšlenější a tudíž i nebezpečnější metody zneužití elektronického bankovnictví. Může se jednat např. o instalaci falešných krytů bankomatů či zneužití internetového bankovnictví pomocí podvodných e-mailů, které mohou páchat jak organizované gangy ze zahraničí, tak i hackeři.

Cílem této diplomové práce je objasnit pojem elektronického bankovnictví a s ním spojené možnosti jeho zneužití. Jelikož lidé nejvíce využívají pouze dva prostředky elektronického bankovnictví a to platební karty a internetové bankovnictví, zaměřím se na jejich popis a hlavně rizika jejich zneužití. Na základě zjištěných skutečností poté navrhnout prostředky k minimalizaci zneužití elektronického bankovnictví.

2 Pojem a historický vývoj elektronického bankovnictví

S nástupem techniky a jejím rozvojem vznikly požadavky na přenášení informací, kterých neustále přibývalo. Začaly se hledat cesty a využívat dostupné prostředky pro vzdálenou komunikaci. První velkou změnu zaznamenal telefon, ale nebyl pro bankovnictví nejspolehlivějším komunikačním prostředkem. Poté se začal využívat fax, ale bohužel technika nebyla nejdokonalejší a tak občas vytištěné příkazy nebyly čitelné a jako prvek zabezpečení se zvolilo potvrzování telefonem. Revoluční zlom nastává v používání počítačů, které umožňují zpracovat všechna data. [1]

Klasické bankovní služby přestávají lidem stačit, jelikož jsou nepružné, pomalé a obírají člověka o čas. Začíná se objevovat elektronické neboli přímé bankovnictví. Přímé bankovnictví patří mezi prostředky vzdáleného přístupu k peněžním hodnotám, při jejichž užívání se vyžaduje identifikace klienta nějakým způsobem na dálku. [2]

„Přímé bankovnictví znamená, že klient může být díky elektronickým prostředkům komunikace se svými penězi v kontaktu 24 hodin denně, 365 dní v roce, až je v zaměstnání, doma, nebo uprostřed oceánu. Zkrátka odkudkoliv a kdykoliv.“[3]

Charakteristické rysy služeb elektronického bankovnictví jsou: [4]

- k poskytování služeb dochází prostřednictvím elektronického kanálu
- na jedné straně je klient s určitým technickým vybavením a na druhé straně je buď přímo automatický systém banky, nebo pracovník obsluhující tento systém
- klient musí být při elektronické komunikaci vždy jednoznačně identifikovatelný a jeho právo vykonat požadovanou operaci je vždy ověřeno určitým autorizačním mechanismem
- nejčastějšími operacemi jsou tuzemský platební příkaz a stav peněz na účtu

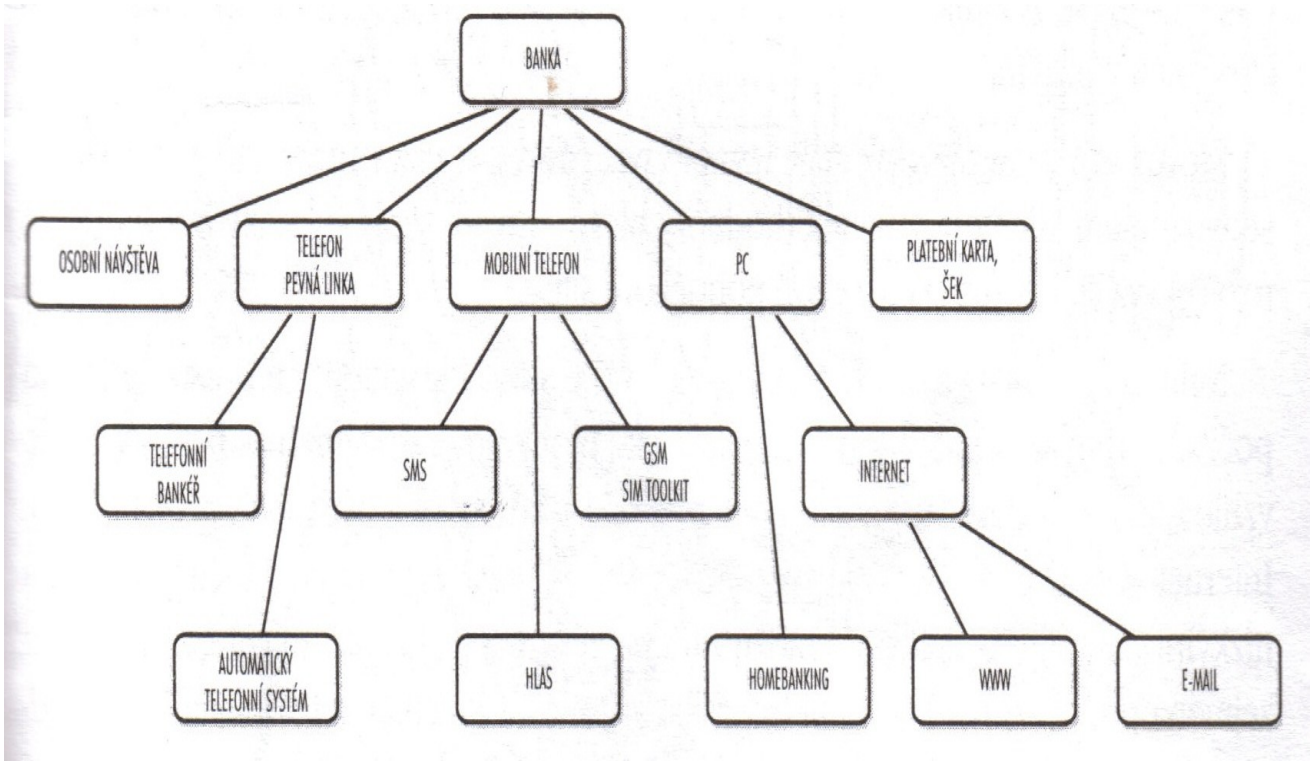
[1] MÁČE, M. *Platební styk – klasický a elektronický*.
[2] Internetové stránky FinExpert. Dostupné z:
<http://finexpert.e15.cz/o-bezpecnosti-primeho-bankovnictvi-s-prof-smejkalem>. [cit. 7. dubna 2011]
[3] PŘÁDKA, M.; KALA, J. *Elektronické bankovnictví*. s. 1
[4] Internetové stránky CEED. Dostupné z:
<http://www.ceed.cz/bankovnictvi/778elektronicke_bankovnictvi.htm>.[cit. 23. února 2011]

Většina bank již řadu let nabízí širokou paletu produktů elektronického neboli přímého bankovnictví. Jedná se o služby, které umožňují komunikaci banky a klienta bez toho, aby klient musel banku navštívit. Vše se děje buď pomocí telefonu, nebo počítače a internetu.[5]

Klient banky se stává prostřednictvím nových komunikačních kanálů, jako jsou mobilní či pevné linky nebo internet, pánem svého času. Komunikovat se svou bankou může 24 hodin denně 7 dnů v týdnu, čímž mu odpadají zdlouhavé návštěvy poboček banky. [6]

Základní formy elektronického bankovnictví jsou platební karty, telefonní bankovnictví (phonebanking), internetové bankovnictví (internetbanking), GSM bankovnictví (bankovnictví poskytované pomocí mobilních telefonů) a homebanking.[7]

Obrázek 2.1 - Možnosti komunikace klienta a banky



Zdroj: PŘÁDKA, M.; KALA, J. *Elektronické bankovnictví*. 1. vydání. s. 5

[5] Internetové stránky Zlatá koruna. Dostupné z:

<http://www.zlatakoruna.info/clanky/21-2-elektronicke-bankovnictvi/14561-co-byste-meli-vedet-o-elektronickem-bankovnictvi>. [cit. 7. února 2011]

[6] MÁČE, M. *Platební styk – klasický a elektronický*.

[7] PŘÁDKA, M.; KALA, J. *Elektronické bankovnictví*.

2.1 Právní úprava

Jelikož došlo k prudkému nárůstu významu elektronického bankovnictví je daná oblast předmětem úpravy na úrovni EU. [8]

Za základní normy lze považovat Směrnici č. 2000/46/ES, o přístupu k činnosti institucí elektronických peněz, jejím výkonu a obezřetnostím dohledu nad touto činností. Cílem této směrnice je zamezit nekontrolovatelné emisi elektronických peněz, zvýšit právní jistotu klienta a prohloubit důvěru veřejnosti k elektronickým platebním prostředkům. [9]

Dále je to Směrnice č. 2002/65/ES, o uvádění finančních služeb pro spotřebitele na trh na dálku a Směrnice č. 97/7/ES, o ochraně spotřebitele v případě smluv uzavřených na dálku, ve kterých je upraven postup při zneužití platební karty. Komise ES vydala doporučení č. 97/489/ES, o operacích prováděných elektronickými platebními prostředky a zejména o vztahu mezi vydavatelem a držitelem, které je zaměřeno především na úpravu mezi vydavatelem a držitelem s akceptem na ochranu práv držitele.[10]

Základní úpravu vztahů v oblasti platebního styku je u nás upravena v zákoně č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku), který implementuje do našeho právního řádu výše uvedené směrnice a do určité míry reflektuje i zmíněná Doporučení. Zákon upravuje provádění převodů peněžních prostředků na území České republiky v české měně a provádění příhraničních převodů. Dále vydávání a užívání elektronických platebních prostředků, vznik a provozování platebních systémů v jakékoliv měně a práva a povinnosti jejich účastníků, jestliže se dohodli, že se tyto platební systémy řídí právním řádem České republiky, a dále některé povinnosti účastníků platebních systémů provozovaných podle právního řádu některého z členského státu Evropské unie a dalších států tvořící Evropský hospodářský prostor. [11]

---

[8] MÁČE, M. *Platební styk – klasický a elektronický*.

[9] Internetové stránky Eur-lex.europa.eu. Dostupné z:
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0046:CS:HTML>.
[cit. 14. února 2011]

[10] Internetové stránky Eur-lex.europa.eu. Dostupné z:
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0065:CS:HTML>.
[cit. 14. února 2011]

[11] Internetové stránky BusinessCenter. Dostupné z:
<http://business.center.cz/business/pravo/zakony/platebni_styk/>.[cit. 25. února 2011]

Další právní úprava je v zákoně č. 140/1961 Sb., trestní zákon, který byl v platnosti do 31. 12. 2009. Tento se zaměřuje také na trestné činy hospodářské, do této oblasti spadá trestný čin §249b Neoprávněné držení platební karty. Tento zákon prošel novou právní úpravou a od 1. 1. 2010 se jedná o zákon č. 40/2009 Sb., trestní zákon. V tomto zákoně je trestný čin §234 Neoprávněné opatření, padělání a pozměnění platebního prostředku.

Trestní zákon č. 140/1961 Sb. definuje § 249b Neoprávněné držení platební karty takto:

„Kdo si neoprávněně opatří nepřenosnou platební karty jiného, identifikovatelnou podle jména nebo čísla, nebo předmět způsobilý plnit její funkci, bude potrestán odnětím svobody až na dvě léta, nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.“[12]

Nová úprava trestního zákonu č. 40/2009 Sb. definuje §234 Neoprávněné opatření, padělání a pozměňování platebního prostředku takto:

„(1) Kdo sobě nebo jinému bez souhlasu oprávněného držitele opatří, zpřístupní, přijme nebo přechovává platební prostředek jiného, zejména nepřenosnou platební kartu identifikovanou podle jména nebo čísla, elektronické peníze, příkaz k zúčtování, cestovní šek nebo záruční šekovou kartu, bude potrestán odnětím svobody až na dvě léta zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo sobě nebo jinému opatří, zpřístupní, přijme nebo přechovává padělaný nebo pozměněný platební prostředek bude potrestán odnětím svobody na jeden rok až pět let.

(3) Kdo padělá nebo pozmění platební prostředek v úmyslu použít jej jako pravý nebo platný, nebo kdo padělaný nebo pozměněný platební prostředek použije jako pravý nebo platný bude potrestán odnětím svobody na tři léta až osm let.“[13]

Jak již bylo zmíněno, došlo k novelizaci trestního zákona a od 1. 1. 2010 platí nový trestní zákon č. 40/2009 Sb. V předešlém zákonu se oblastí zneužívání elektronického bankovnictví zabýval pouze §249b Neoprávněné držení platební karty a tudíž se zaměřoval pouze na platební karty. V novém trestním zákoně č. 40/2009 Sb. je §234 Neoprávněné opatření, padělání a pozměňování platebního prostředku. Zde jsou zahrnuty jak platební karty, tak veškeré platební prostředky.

---

[12] Trestní zákon 140/1961 Sb.

[13] Trestní zákon č. 40/2009 Sb.

2.2 Platební karty

Platební karty jsou jednou z nejpopulárnějších metod používaných k provádění bezhotovostních transakcí. V České republice jsou vydávány teprve několik let, ale i tak zde zcela zdomácněly, a málokdo si bez nich umí představit běžný, každodenní život. Staly se prostředkem, jak se bezpečně a pohodlně dostat k financím na svém účtu, platit v obchodech, jak kamenných, tak internetových doma i v zahraničí, nebo získat úvěr. [14]

S platební kartou můžeme provádět dvě základní věci – platit za zboží a služby nebo vybírat hotovost z bankomatu. Ostatní operace jsou považovány za druhotné. [15]

2.2.1 Historický vývoj platebních karet

První platební karta spatřila světlo světa již před několika desetiletími a to zejména v západní Evropě a severní Americe. Jejich vývoj je spjat s šedesátými léty.

U nás byla situace jiná. První bankomat jsme spatřili v roce 1988 a až druhá polovina devadesátých let je spjat s větším rozšířením a zejména aktivním používáním platebních karet.

Za kolébku platebních karet se považují Spojené státy americké. Prvními předchůdci byli cestovní šeky, peněžní poukázky a úvěrové známky. Všechny tyto produkty sloužily pro potřebu bezpečného placení za zboží a služby, bezpečné přenesení peněz na dálku, zvýšení prodeje na obchodní úvěr a snadná identifikace zákazníků a s tím spojená evidence jejich nákupu. [15]

Za předchůdce platební karty je považována tzv. věrnostní karta, kterou jako první vydala v roce 1914 americká telegrafní společnost Westen Union Telegraph Company. Její zákazníci tak mohli bez okamžitého placení telefonovat a zasílat telegramy. Stačilo pouze předložit kartu a podepsat účet, měsíční vyúčtování klient obdržel poštou. Důvodem proč společnost začala vydávat tyto karty, byla snaha si udržet dobré zákazníky v době rostoucí konkurence a přimět je k častějšímu používání služeb. Proto se tyto karty nazývají věrnostní platební karty.[16]

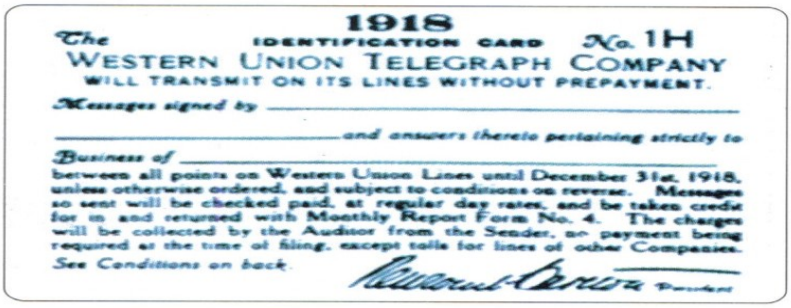
---

[14] Internetové stránky Platební–karty.info. Dostupné z <http://platebni-karty.info/index.php>. [cit. 4. února 2011]

[15] PŘÁDKA, M.; KALA, J. *Elektronické bankovnictví*.

[16] JUŘÍK, P. *Platební karty – velká encyklopedie 1870 - 2006*.

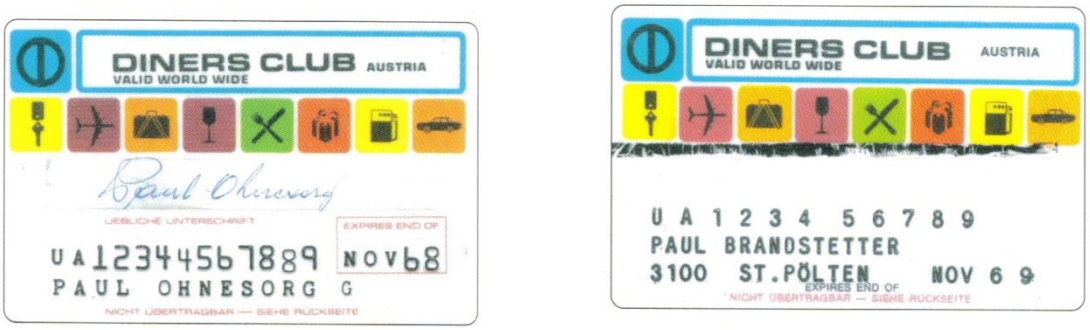
Obrázek 2.2 - První platební karta na světě



Zdroj: JUŘÍK, P. *Platební karty – velká encyklopedie 1870 – 2006*. 1. vydání. s 21

Universálně použitelnými se roku 1950 v USA staly karty Diners Club International. K jejímu vzniku se váže zajímavá historka. Jednoho lednového večera roku 1949 byl Frank McNamara na obchodní večeři se svými obchodními partnery v newyorské restauraci. Když vrchní po večeři přinesl účet, McNamara začal hledat peněženku a zjistil, že ji nechal v druhém saku. Protože ho v restauraci znali, nabídli mu, aby zaplatil příště, ale on telefonoval manželce a ta mu hotovost přinesla. Nepříjemná situace ho vedla k otázce, proč by měli být lidé v restauraci omezeni hotovostí, kterou mají zrovna u sebe. Napadlo ho založit klub nazývaný Diners Club (diners – večeře) a úkolem klubu bylo vydávat členům klubu úvěrové karty. Tyto karty již umožňovali zaplatit v restauracích, hotelech a obchodech, které se společností, jež karty vydávala, uzavřeli smlouvu. Zde také došlo poprvé k zaúčtování ročního poplatku za vydání a správu karty, který hradil držitel karty. V roce 1951 tyto karty začali akceptovat také obchodníci v Kanadě a na světě byla první mezinárodní platební karta.[17]

Obrázek 2.3 - První univerzální karty Diners Club



Zdroj: JUŘÍK, P. *Svět platebních a identifikačních karet*. 2. vydání. s. 178

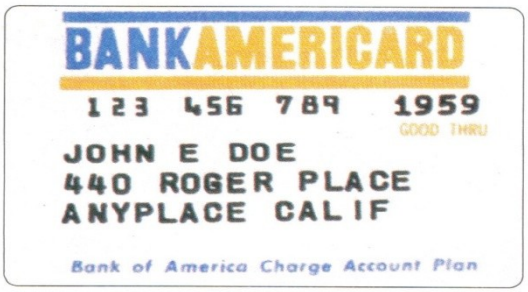
[17] JUŘÍK, P. *Platební karty – velká encyklopedie 1870 - 2006*.

Koncem 40. let se o platební karty začaly zajímat i americké banky. v roce 1947 zavedla newyorská banka Flatbush Nationa Bank of Brooklyn papírový doklad nazvaný „Charg-It“, který sloužil k placení v lokální síti obchodů. Podobné katry poté zavedlo několik dalších amerických bank a všechny tyto karty sloužily pouze k placení, nikoli k čerpání úvěru.

První kreditní katru vydala v roce 1951 newyorská banka The Franklin National. Tato karta byla vydávána zdarma a klienti museli uhradit své provedené nákupy do 30, 60 nebo 90 dnů. Během několika let katry vydávala asi stovka amerických bank. [18]

V roce 1966 pronikl systém Bank Americard do Evropy. První neamerický vydavatel byla Barclays Bank ve Velké Británii, kterou následovalo více jak 21 000 bank po celém světě. [19]

Obrázek 2.4 - První úspěšná bankovní karta



Zdroj: JUŘÍK, P. *Svět platebních a identifikačních karet*. 2. vydání. s 178

V první polovině 70. let banky objevily možnosti magnetického proužku a začaly budovat sítě bankomatů a platebních terminálů. V 80. letech začaly banky investovat do vývoje čipových karet a platební katry v podobě debetní karty k běžnému účtu se poté staly samozřejmou součástí nabídky bankovních služeb. [19]

V České republice jsou mezinárodní platební karty přijímány od roku 1969, jako první se jednalo o karty Diners Club a American Express. Akceptace platebních karet v České republice fungovala dlouho před tím, než u nás byla první platební karta vydána. Jediné karty, které se zde před pádem komunismu vyskytovaly, byly v rukou cizinců. A jediná společnost, která přišla do styku s cizinci, byla cestovní kancelář Čedok – spadaly pod ní všechny

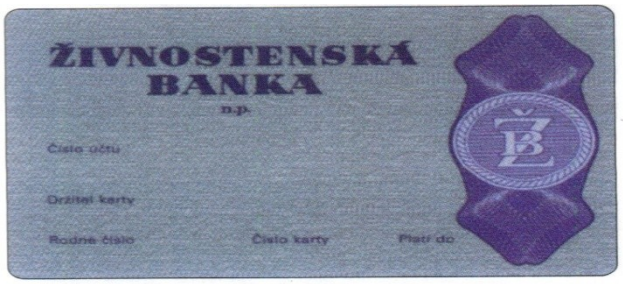
[18] JUŘÍK, P. *Svět platebních a identifikačních karet*.

[19] JUŘÍK, P. *Svět platebních a identifikačních karet*.

subjekty působící v oblasti cestovního ruchu. Proto byl akceptací platebních karet pověřen právě Čedok. [20]

První platební kartu na území tehdejšího Československa vydala roku 1988 Živnostenská banka jako dispoziční kartu k tuzexovému účtu, která sloužila k výběru odběrních poukazů PZO Tuzex a v pobočkách ČSOB A SBČS a k bezhotovostnímu placení v prodejnách Tuzex. V roce 1991 vydala první VISA kartu u nás.[20]

Obrázek 2.5 - První platební karta v Československu



Zdroj: JUŘÍK, P. *Svět platebních a identifikačních karet*. 2. vydání. s 179

V bývalém Československu byla problematika vydávání platebních a bankomatových karet náplní Usnesení vlády ČSSR č. 17/1985 a řady jednání tzv. Mezinárodní komise expertů. V té době již vydávala první platební karty v bývalém RVHP Spořitelna města Berlína, která instalovala několik bankomatů vyrobených firmou Robotron. První bankomatové karty vydaly Česká a Slovenská státní spořitelna v létě roku 1989.[21]

Obrázek 2.6 - První bankomatová karta České státní spořitelny

Zdroj: JUŘÍK, P. *Svět platebních a identifikačních karet*. 2. vydání. s 179

[20] Internetové stránky Peníze. cz. Dostupné z: <http://www.penize.cz/platebni-karty/16363-cedok-tuzex-a-cesky-karetni-boom>.[cit. 4. ledna 2011]

[21] JUŘÍK, P. *Svět platebních a identifikačních karet*.

2.2.2 Ochranné prvky

Emitenti platebních karet se brání jejich zneužití různými způsoby. Ty lze rozdělit na dvě hlavní skupiny, a to na technickou ochranu obdobou technickým ochranám na „klasických“ dokladech a na ochranu elektronických údajů zakódovaných v elektronickém prvku platební karty. [22]

První skupina ochranných prvků spočívá např. v umístění hologramu v ploše platební karty, použití speciálních tiskových technik, použití speciálních podtisků, které znemožní přepsání podpisového pole na platební kartě (při přepsání podpisu se např. v podpisovém poli objeví slovo VOID, tj. neplatný), použití prvku viditelných pouze v dopadajícím ultrafialovém či jiném záření a další techniky, použitelné na základě rozhodnutí emitenta. Někdy mohou být také zařazeny i utajované prvky, které jsou známy omezenému okruhu osob, zpravidla pouze z okruhu nejvyššího managementu emitenta nebo jeho bezpečnostního pracoviště.[23]

Do skupiny ochranných prvků patří i přesné dodržování normovaných rozměrů platebních karet, které je dáno mezinárodním standardem. Platební karty se vyrábí z odolných plastů a mívají standardní rozměry, délka karty je 85,595 mm, šířka 53,93 mm a její tloušťka 0,76 mm. Tyto rozměry stanoví mezinárodní norma ISO 7810. Karta odlišných rozměrů není příslušným snímacím zařízením akceptována. Základním ochranným prvkem každé platební karty je její číslo, které je jedinečné. Kromě tohoto kódu má každá karta na zadní straně magnetický proužek, na kterém jsou uložena podstatná data. Jelikož většina uživatelů, kteří platí platebními kartami na internetu, nemá čtečku kreditních karet, je na kartách umístěn ještě jeden dodatečný prvek. [23]

Tomuto prvku se říká Card Verification Value, případně Card Vecification Code, zkráceně CVV nebo CVC. Tímto kódem je dodatečné číslo, které je na kartách MasterCard, Visa a Discover umístěno na zadní straně u podpisového vzoru. Užívá se pro zvýšení ochrany před zneužitím při elektronickém převodu peněz. Podle čísla karty lze rozeznat mnoho věcí.

---

[22] SADOVSKÝ, Dalibor; SUCHÁNEK, Jaroslav. Platební karty a možnosti jejich zneužití. Kriminalistika [online]. 2004, č. 1 [cit. 9. února 2011]. Dostupné z: <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0401/suchanek_info.html>.

[23] SADOVSKÝ, Dalibor; SUCHÁNEK, Jaroslav. Platební karty a možnosti jejich zneužití. Kriminalistika [online]. 2004, č. 1 [cit. 9. února 2011]. Dostupné z: <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0401/suchanek_info.html>.

První dvě číslice určují druh karty (např. VISA začíná vždy číslem 4), dalších pět číslic představují vydavatele karty (banku), zbytek čísel je určen pro konkrétního držitele karty. [24]

Do uvedené skupiny ochranných prvků lze zařadit i embosované (vytlačené) znaky, které mají převážně charakter písmen nebo číslic (ale i jiných znaků, jako např. hvězdičky, geometrické obrazce, diakritická znaménka, apod.). Embosované znaky jsou v platebních kartách vytvářeny působením tepelného zdroje, který má tvar požadovaného znaku a vzhledově jsou tvořeny vystouplými znaky na lícové straně karty a naopak zahloubenými znaky na rubové straně karty. Základ (nosič) platební karty je tvořen termoplastickými hmotami, které umožňují svými vlastnostmi při vhodném lokálním zahřátí vytvoření zmíněných znaků. Základ platební karty může být tvořen několika navzájem barevně odlišnými vrstvami (třemi až šesti), které při vytvoření embosovaných prvků umožňují jejich barevnou odlišnost od převažující barvy podkladu karty.[24]

Nosič platební karty podléhá opotřebovávání při jejím používání, které se týká i opotřebení magnetického proužku. Uplatňuje se i stárnutí a změna vlastností plastického materiálu a zvyšuje se tím riziko poštu odmítnutých transakcí. [24]

Druhá skupina ochranných prvků platebních karet se týká elektronických údajů. Elektronické údaje umístěné na magnetickém proužku, případně na mikročipu, musí být umístěna na přesně vymezeném místě platební karty. Elektronické prvky včetně údajů v nich zakódovaných jsou na polotovar platební karty umisťovány dodatečně, až po vytvoření nosiče karty a umístění ochranných prvků první uvedené skupiny. Individualizace elektronicky kódovaných informací je prováděna až bezprostředně před konkrétním vydáním karty oprávněnému uživateli tzv. nahráním. [24]

Platební karty jsou opatřeny magnetickými proužky, které v elektronické podobě zachycují veškeré potřebné údaje. Některé z údajů jsou otevřené, tedy nekódované, jiné jsou různými způsoby kódované a znemožňují tak zneužití těchto karet.

Oprávněný přístup k operacím s platebními kartami je vždy omezen zadáním příslušného číselného kódu (zpravidla čtyřmístného), který má za povinnost oprávněný uživatel udržovat v tajnosti (jedná se o tzv. PIN – Personal Identification Number. [24]

---

[24] SADOVSKÝ, Dalibor; SUCHÁNEK, Jaroslav. Platební karty a možnosti jejich zneužití. Kriminalistika [online]. 2004, č. 1 [cit. 9. února 2011]. Dostupné z:

<http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0401/suchanek_info.html>.

Užití karty je možné tedy pouze v případě, že uživatel zná všechny tyto vlastnosti karty. Číslo karty, jméno vlastníka karty, platnost platební karty, případně kód CBC, či podpisový vzor, podle způsobou platby. [24]

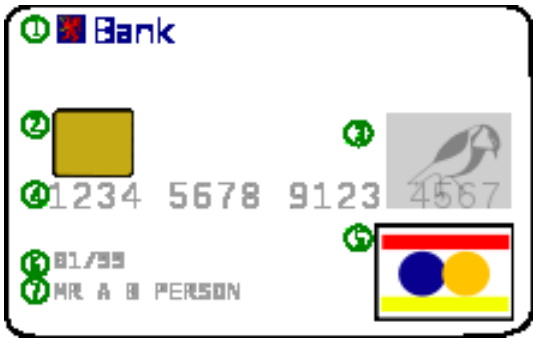
Platební karty je majetkem banky, která ji vydala, nikoli držitele karty. Proto peněžní ústavy většinou vyžadují její vrácení po skončení doby platnosti.

Bezpečnostní prvky na klasické platební kartě: [25]

Přední strana obsahuje:

- Logo banky
- EMV čip
- Hologram
- Číslo kreditní karty
- Logo vydavatele
- Platnost karty
- Jméno majitele

Obrázek 2.7 – Přední strana platební karty

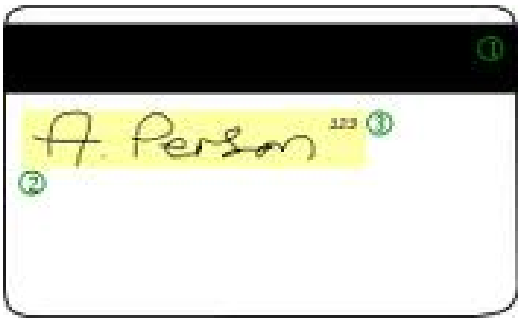


Zdroj: Internetové stránky Wikipedia. Dostupné z: <http://cs.wikipedia.org/wiki/Platebn%C3%AD_karta>. [cit. 3. ledna 2011]

Zadní strana obsahuje:

- Magnetický proužek
- Podpisový vzor
- Kód CVC

Obrázek 2.8 – Zadní strana platební karty



Zdroj: Internetové stránky Wikipedia. Dostupné z: <http://cs.wikipedia.org/wiki/Platebn%C3%AD_karta>. [cit. 3. ledna 2011]

[25] Internetové stránky Wikipedia. Dostupné z: <http://cs.wikipedia.org/wiki/Platebn%C3%AD_karta>.[cit. 3. ledna 2011]

2.2.3 Dělení platebních karet

V průběhu své historie se platební karty rozdělily na řadu druhů, které veřejnosti splývají do názvu kreditní nebo platební karta. Karty dělíme do několika skupin a to podle:[26]

- způsobu zúčtování transakcí – kreditní karty, debetní karty, charge karty
- druhu záznamu dat – embosován karty, karta s magnetickým záznamem, čipová karta
- způsobu použití – platební karty, bankomatové karty, šekové záruční karty
- rozsahu použití – síť vydavatele, regionální, vnitrostátní, mezinárodní
- uživatele – osobní karty, služební karty, bez identifikace
- marketingu – základní karty, prestižní karty, výběrové karty.

Členění karet podle způsobu zúčtování transakcí:

- kreditní karta – banka prostřednictvím této karty poskytuje klientovi možnost čerpání spotřebitelského úvěru, klient ji může také použít k zaplacení za zboží a služby i k výběru hotovosti z bankomatu. Klient si od banky půjčuje peníze a tento úvěr je následně včetně úroků splácen.
- debetní karta – karta je vydána k běžnému účtu, držitel s ní uhrazuje platby za zboží a služby nebo vybírá hotovost z bankomatu, při platbě klient čerpá vlastní prostředky, nejprve je daná částka zablokována a až dojde k účetnímu vypořádání obchodu, banka ji z klientova účtu odepíše, někdy je ale umožněn též kontokorentní úvěr
- charge karta – tato karta je historicky nejstarší typ platební karty, obdoba kreditní karty, tuto katru lze porovnat s placením „na fakturu“. Vydavatel karty klientovi po určité době sečte všechny čerpané položky a pošle fakturu na jejich uhrazení.

Členění karet podle záznamu dat:

- embosován karta – také umožňuje výběr z bankomatu jako elektronická platební karta, ale prostřednictvím této karty lze platit na více obchodních místech, opatřenými buď elektronickým pokladním terminálem, nebo sprinterem

[26] JUŘÍK, P. *Svět platebních a identifikačních karet*.

(mechanickým snímacím zařízením sloužícím k provedení otisku platební karty a identifikačního štítku obchodníka na prodejní doklad)

- karta s magnetickým proužkem – data (identifikační údaje a data o provedených transakcích) jsou zaznamenávána na magnetický proužek. Toto umožňuje provádění elektronických transakcí platební kartou.
- čipová karta – data jsou zaznamenána v mikročipu, který je umístěn na přední straně katry. Tyto katry mají určité výhody a to ve vyšším stupni zabezpečení, možnosti širšího využití, které umožňuje paměť čipu a možnost lokálního ověření identifikačních údajů držitele (např. PIN) na rozdíl od ověření online transakcí

2.3 Internetové bankovnictví

Internetové bankovnictví neboli také internetbanking je metoda kontaktu klienta s bankou pomocí webového rozhraní. Jako komunikační prostředek se zde využívá počítač. Platební styk přes internet umožňuje komunikaci klienta banky prostřednictvím počítače připojeného na celosvětovou síť internet. Na internetu se zadá www adrese banky, kde klient zadá uživatelské jméno a certifikační kód, a dostane se na speciální stránky banky. Zde může provádět různé operace. Vše provádí s autorizačním klíčem, který zajišťuje zabezpečení proti zneužití. Z hlediska klienta je výhodou rychlý a snadný přístup k účtu, z hlediska banky úspora pracovníků na přepážkách. [27]

Protože prostředí sítě internet nemusí být bezpečné, snaží se banky zajistit při své komunikaci s klientem maximální ochranu přenášených dat. K zabezpečení operací slouží speciální kód generovaný autentizačním kalkulátorem či zaslaný na mobilní telefon. Alternativou jsou certifikáty sloužící k ověření klienta a banky. Komunikace s bankou je v síti internet kódována. [28]

2.3.1 Historie internetového bankovnictví

Prvním průkopníkem internetového bankovnictví byla v polovině 90. let 20. století Rodinná záložna, ta však zkrachovala. Poté pomyslné žezlo převzala dodnes působící družstevní záložna Fio a nabídla internetového bankovnictví všem svým klientům. Převzetím

---

[27] MÁČE, M. *Platební styk – klasický a elektronický*.

[28] Internetové stránky Zlatá koruna. Dostupné z: <http://www.zlatakoruna.info/clanky/21-2-elektronicke-bankovnictvi/14561-co-byste-meli-vedet-o-elektronickem-bankovnictvi>. [cit. 7. února 2011]

licence Zemské banky začala 4. května 1998 oficiálně působit Expandia Banka (dnešní eBanka) a jako první banka nabídla plné ovládání účtu přes internet. Její práce byla motivem pro ostatní banky k nabízení vlastního internetového bankovnictví. [29]

V době, kdy eBanka začala rozvíjet další etapu internetbankingu, se postupně začaly v Česku rozhoupávat k investicím do rozvoje internetbankingu i další finanční instituce. Většina tuzemských bank, než se odhodlala umožnit klientům ovládání účtu přes internet, zřizovala spíše call centra a sháněla telefonní operátory. [29]

Z velkých bankovních domů se k zavedení internetového bankovnictví jako první odhodlala zavést Komerční banka. Učinila tak na začátku nového tisíciletí v roce 2000. Další dvě velké banky, ČSOB a Česká spořitelna internetbanking rozjely shodně v roce 2002. [29]

2.3.2 Způsoby zabezpečení internetového bankovnictví

Aby mohlo internetové bankovnictví bezpečně fungovat, je třeba ošetřit několik oblastí. Jedná se především o identifikaci banky klienta, zabezpečení přenosu dat a také o bezpečnost klientského počítače. [30]

Identita banky je ověřována tzv. SSL certifikátem, který bance vydává nezávislá instituce. Klient má tedy jistotu, že stránky, jejichž prostřednictvím komunikuje s bankou, patří skutečně jí. Přenos citlivých dat je ve všech bankách řešen SSL šifrováním (ikona žlutého visacího zámku na stavové liště). [30]

Identifikace klienta, někdy je také používán termín autentizace, může být zajištěna několika způsoby, viz níže. Jedná se o ověření totožnosti osoby, která vstupuje do informačního systému. Autentizace uživateli umožní pouze pasivní operace (např. zjištění zůstatku účtu) a jestliže chce provést nějakou aktivní operaci (např. platební příkaz) musí ji navíc potvrdit zadáním dalších údajů. 30

- **Uživatelské jméno (číslo) a heslo** – jedná se o obecně nejběžnější a nejznámější způsob autentizace. K potvrzení identity stačí uživateli internetového bankovnictví znát tyto dva údaje, což je pro uživatele sice nenáročná, ale ne příliš bezpečná metoda. Zjistí-li tyto údaje cizí osoba, získá tak neomezený

[29] Internetové stránky Peníze.cz. Dostupné z: <http://www.penize.cz/prime-bankovnictvi/42614-odkud-kam-miri-cesky-internetbanking>. [cit. 4. ledna 2011]

[30] Internetové stránky Peníze.cz. Dostupné z: <http://www.penize.cz/bezne-ucty/18366-internetove-bankovnictvi-jsou-vase-penize-v-bezpeci>. [cit. 11. února 2011]

přístup k účtu klienta a banka nemá šanci poznat, že se nejedná o správného uživatele. I v případě, že je jméno a heslo pečlivě střeženo, může být účet napaden. Existují programy, které umí tzv. odečítat z klávesnice či odposlouchávat a šikovný hacker si údaje dokáže snadno zjistit.

- **SMS klíč** – jedná se o jednorázové heslo pro konkrétní operaci, které banka zašle na mobilní telefon. Transakce je provedena až poté, co je tento potvrzovací kód opsán do systému internetového bankovnictví.
- **Autorizační kalkulátor** – je drobné elektronické zařízení, které dokáže generovat jednorázová hesla pro potvrzení operací. Kalkulátor funguje na podobném principu jako SMS klíč, je přenosná a chráněna čtyřmístným heslem. Po zadání hesla a stisknutí příslušného tlačítka vygeneruje šestimístný kód, který klient aplikuje pro vstup do internetového bankovnictví.
- **Elektronický podpis** – pro komunikace s použitím elektronického podpisu je nutný tzv. certifikát vydávaný autorizovanou certifikační autoritou. Certifikát má podobu souboru a může být uložen na přenosném médiu (USB flash disku, CD). Nikdy by neměl být uložen na harddisku volně přístupného počítače, protože by mohl být zkopírován

Obrázek 2.9 zobrazuje přehled zabezpečení aktivních operací u jednotlivých bank. Nejčastější je zabezpečení prostřednictvím SMS kódu, certifikátu či PIN kalkulátoru. SMS kód je platný pouze pro právě uskutečňovanou operaci a přichází na vyžádání klienta na jeho mobilní telefon ve formě SMS.

Obrázek 2.9 – Zabezpečení aktivních operací jednotlivých bank

Banka	Produkt	Zabezpečení aktivních operací	Způsob zabezpečení
BAWAG Bank	Bawag direct	ANO	certifikát
Citibank	Citibank online	NE	
Česká spořitelna	Servis 24 Internetbanking	ANO	SMS, PIN kalkulátor
ČSOB	Internetbanking 24	ANO	čipová karta, SMS
eBanka		ANO	SMS, PIN kalkulátor, certifikát
GE Money Bank	Internet banka	dle výše částky	digitální podpis
HVB Bank	Online Banking	ANO	PIN kalkulátor
Komerční banka	Mojebanka	ANO	SMS
Poštovní spořitelna	Max Internetbanking PS	ANO	SMS
Raiffeisenbank	Internetové bankovnictví	ANO	certifikát, SMS
Volksbank	Internet banking	ANO	certifikát
WSPK	Internetbanking	ANO	certifikát, iKey token
Živnostenská banka	Net banka	ANO	SMS

Zdroj: Internetové stránky Měšec. Dostupné z: <http://www.mesec.cz/clanky/jak-je-zabezpecene-internetove-bankovnictvi//>.[cit. 24. února 2011]

2.4 Telefonní bankovnictví

Dalším základním nástrojem je telefon a s ním spojené telefonní bankovnictví neboli také phonebanking. Phonebanking je platební styk založený na komunikaci s bankou prostřednictvím telefonu tak, že klient komunikuje hlasem s živými pracovníky banky nebo tlačítky buď s živým operátorem banky, nebo hlasovým informačním systémem.

Telefonní bankovnictví je po platební kartě historicky druhým přímým komunikačním kanálem, který se dočkal masovějšího rozšíření.

V době kdy telefonní bankovnictví vznikalo, nebyly ještě informační technologie na takovém stupni rozvoje, aby se vše dalo plně zautomatizovat. Dříve si pod tímto pojmem člověk většinou představil živého telefonního bankéře či bankéřku, která někde v telefonickém centru (call centru) vyřizuje požadavky klientů. Dnes to tak ale nemusí být, většinu činností, které dříve vyřizoval člověk, dnes může převzít počítač.

Princip této služby je jednoduchý. Klient zavolá na linku telefonního bankovnictví. U většiny bank je toto číslo bezplatné a lze na něj volat i z mobilního telefonu. Klient se prokáže svým identifikačním číslem a číslem PIN. Tato služba se vyskytuje ve dvou verzích. U první verze klient komunikuje s automatickým hlasovým systémem. Zde získává informace o produktech, o aktuálním zůstatku, ale také zadává příkazy k úhradě či inkasu, trvalé příkazy, provádí konverzi měn. Ve druhé verzi klient komunikuje s telefonním bankéřem, který poskytuje stejné služby jako pracovník na přepážce od zadávání příkazů po zadávání termínovaných vkladů. Nevýhodou je, že mimo pracovní dobu klient komunikuje jen s hlasovým systémem. [31]

Přístup do systému je vázán na zadání čísla PIN, případně hesla. Pokud dojde k vyzrazení těchto čísel, je celý systém poměrně lehce zneužitelný. Nebezpečí ale není zase tak veliké, neboť systém pracuje pouze s bezhotovostním platebním stykem a zpravidla lze operovat pouze s omezenou částkou. Veškerá komunikace je bankou zaznamenána a archivována, proto je snadné dohledat podezřelé operace. [31]

2.5 GSM banking

Nástup mobilních telefonů digitálního standardu GSM znamenal v mnoha směrech revoluci.

Platební styk, který je založen na komunikaci s bankou prostřednictvím mobilních telefonů, která může být založena: [32]

- prostřednictvím šifrovacích SMS zpráv
- prostřednictvím technologie SIM Toolkit
- s využitím technologie WAP

Klienti mohou odesílat z mobilních telefonů pomocí SMS zpráv, v přesně nadefinovaných formátech, požadavky k získání informací nebo příkazy k provedení a banky jim zpět odešle odpověď SMS zprávou obsahující požadovanou informaci. Výhodou je použitelnost u všech mobilních telefonů, bez ohledu na operátora. Komunikace probíhá pouze

---

[31] Internetové stránky Zlatá koruna. Dostupné z:

<http://www.zlatakoruna.info/clanky/21-2-elektronicke-bankovnictvi/14561-co-byste-meli-vedet-o-elektronickem-bankovnictvi>. [cit. 7. února 2011]

[32] MÁČE, M. *Platební styk – klasický a elektronický*.

prostřednictvím SMS zpráv. Na první pohled to sice nevypadá příliš bezpečně, ale banka k této aplikaci může vydávat tzv. autentizací kalkulátor, s jehož pomocí si vygeneruje speciální kód, který se poté vloží do struktury SMS zprávy. Nevýhodou je složitější manipulace, protože SMS zprávy musí být odeslány přesně ve formátu daném bankou.[33]

Obrázek 2.9 - Jednorázový příkaz k úhradě:

PLAT_z účtu*kód měny_na účet*kód banky_částka*desetinná místa_měna_konstantní_variabilní_specifický_Klientské číslo_certifikační kód

(např.
PLAT_123456*11_1236547*2400_15000*00_11_558_9_0_065641230_1234567890)

Zdroj: PŘÁDKA, M.; KALA, J. *Elektronické bankovnictví*. 1. vydání.

Komunikace klienta s bankou prostřednictvím technologie SIM Toolkit vyžaduje v mobilním telefonu katru s aplikací od banky. Zde banka do mobilního telefonu (na SIM kartu) nahraje vlastní bankovní aplikaci, která se objeví v menu telefonu. Při nahrávání aplikace je SIM karta zašifrována a nelze z ní získat žádné údaje, ani když dojde ke ztrátě či krádeži telefonu. Přístup k této aplikaci je chráněn zvláštním bankovním PIN, který se nazývá BPIN. Po zadání všech požadovaných údajů vytvoří aplikace zašifrovanou zprávu, kterou dokáže rozšifrovat pouze speciální software v bance. Poté je tato zpráva automaticky zaslána na určené telefonní číslo do banky. Zde je transakce přenesena do systému a banka odešle SMS zprávu o přijetí ke zpracování.[33]

Služba WAP je založena na komunikaci po internetu pomocí protokolu WAP. Jedná se o kombinaci telefonního a internetového bankovnictví. Tato služba umožňuje spojení s bankovním účtem prostřednictvím mobilního telefonu vybaveného technologii WAP. Pomocí mobilního telefonu a autorizačního klíče může klient zadávat např. příkazy k úhradě, zjišťovat zůstatek na účtu i jeho historii apod. [33]

2.6 Homebanking

Jedná se o způsob komunikace klienta a banky za pomocí osobního počítače vybaveného speciálním softwarem, přičemž samostatný přenos dat probíhá většinou prostřednictvím telefonní linky a modemu. Produkt umožňuje obsluhovat účet pomocí počítače připojeného k internetu a softwaru, který je dodán bankou (obvykle instalační CD).

[33] MÁČE, M. *Platební styk – klasický a elektronický*.

Software si klient nainstaluje z CD do počítače, připojí se na internet a může zajišťovat základní služby jako je např. příkaz k úhradě, trvalé příkazy apod. Výhodou je, že tyto produkty bývají kompatibilní s účetními a ekonomickými programy, ale nevýhodou je, že lze používat pouze počítat, kde je program nainstalován. [34]

Homebanking nabízí nejlepší systém zabezpečení ze všech forem elektronického bankovnictví. Přenášení do sítě banky probíhá pomocí hesla uživatele a autorizačního certifikátu. Vzájemná komunikace mezi bankou a klientem je navíc kódována. [34]

[34] Internetové stránky Zlatá koruna. Dostupné z: <http://www.zlatakoruna.info/clanky/21-2-elektronicke-bankovnictvi/14561-co-byste-meli-vedet-o-elektronickem-bankovnictvi>. [cit. 7. února 2011]

3 Možnosti zneužití elektronického bankovnictví

Není platebního prostředku, aby k němu neexistovaly padělky a nedělaly se s ním podvody. Při bezhotovostních platbách se spotřebitelé často chovají velmi neopatrně či nezodpovědně. Asi bychom na ulici neznámé osobě nedali do rukou svou peněženku s hotovostí, aby nám šla koupit noviny, než si vykouříme cigaretu, či dočteme noviny. Při bezhotovostních platbách se však takto někdy chováme. [35]

3.1 Podvody s platebními kartami

Platební karty patří k moderním platebním prostředkům, které jsou celosvětově rozšířeny. Umožňují nám různé způsoby bezhotovostních plateb, výběr peněžních částek v hotovost a další finanční transakce, které lze s jejich pomocí uskutečňovat. Kromě mnoha kladů mají platební karty i své negativní stránky, které jsou nejčastěji spojovány s možností jejich zneužití. [36]

Podvodná jednání spojená s platebními kartami vedou k vysokým finančním ztrátám, jak na straně klientů, tak emitentů. Průběžně jsou prováděna preventivní organizační a technická opatření s cílem omezení ztrát, ale nikdy nelze vyloučit možnost nového, dosud neznámého způsobu páchání trestné činnosti s platebními kartami.[36]

Extrémní způsob spočívá v uplatnění tzv. „bílého platu“. Jedná se o zneužití atrapy platební karty bez jakýchkoliv ochranných prvků nebo elektronických údajů. Ve skutečnosti se jedná pouze o podložku z plastické hmoty, která svými rozměry odpovídá platební kartě, ale je opatřena embosovanými údaji vyřezanými z jiné karty a do falsifikátu platební katy vlepenými. Embosované údaje jsou převzaty z jiné, často odcizené platné platební karty nebo obdobné karty sloužící podobným, nikoliv však platebním účelům, jako jsou např. věrnostní karty různých prodejních řetězců. [36]

---

[35] Internetové stránky Sdružení českých spotřebitelů.

Dostupné z: <http://www.prevencepodvodu.cz/platebni-prostredky/bezhotovostni-platby/bankomat-atm.php>. [cit. 9. února 2011]

[36] SADOVSKÝ, Dalibor; SUCHÁNEK, Jaroslav. Platební karty a možnosti jejich zneužití.

Kriminalistika [online]. 2004, č. 1 [cit. 9. února 2011]. Dostupné z: <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0401/suchanek_info.html>.

Takovýto falzifikát lze uplatnit (ale pouze s vědomím nebo tichým souhlasem příjemce – prodavače, tedy nekorektního obchodníka) při koupi různého zboží v obchodech, které jsou vybaveny pouze čtečkami embosovaných údajů (někdy také nazývány „žehličky“). [37]

Podvody s platebními kartami lze rozdělit na dvě skupiny a to podle toho, zda je trestná činnost páchána oprávněným držitelem platební karty, nebo zda tuto trestnou činnost spáchal neoprávněný držitel platební karty.[37]

3.1.1 Podvody páchané oprávněným držitelem platební karty

Trestná činnost páchaná oprávněným držitelem platební karty se většinou projevuje ve dvou druzích. Jedná se o insolvenci (platební neschopnost) držitele a tzv. simulovanou krádež nebo ztrátu platební karty. [37]

- **Insolvence (platební neschopnost) držitele –** ze strany držitele platební karty se jedná o předem připravený podvod. Platební kartu, nejčastěji kreditního typu užívá tak, že přečerpá zůstatek na účtu a následně nehodlá vzniklé dluhy uhradit. Odhalení pachatele většinou nečiní potíže. Preventivně se těmto problémům emitenti platebních karet brání pečlivým vyhodnocením solventnosti žadatelů o vydání platební karty i využívaní interních databází „problémových klientů“
- **Simulovaná krádež nebo ztráta platební karty –** podstatou je simulovaná krádež či ztráta platební karty, kterou držitel stanoveným způsobem emitentovi ohlásí, ale kartu používá dále, uskutečňuje nekorektní operace, které přisuzuje fiktivnímu pachateli. Tyto neoprávněné finanční operace jsou možné pouze po omezenou dobu (většinou je to do doby blokace platební karty, která trvá v řádu hodin), případně tzv. podlimitními transakcemi, které není potřeba autorizovat.

3.1.2 Podvody páchané neoprávněným držitelem platební karty

Trestná činnost spáchána neoprávněným držitelem platební karty má několik podob:

- **Zneužití karty cizí osobou –** neboli nepoctivý nálezce platební karty. Platební kartu zneužije před jejím zablokováním, např. využitím platného PIN kódu,

---

[37] SADOVSKÝ, Dalibor; SUCHÁNEK, Jaroslav. Platební karty a možnosti jejich zneužití. Kriminalistika [online]. 2004, č. 1 [cit. 9. února 2011]. Dostupné z: <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0401/suchanek_info.html>.

který u platební karty nalezl a to především výběrem hotovosti z bankomatu. Velmi důležité je, aby držitel karty kontroloval, zda ji stále vlastní. V případě její ztráty nebo krádeže by měl neprodleně informovat svoji banku, ta pak provede tzv. stoplistaci karty (blokaci karty). Odpovědnost za ztráty způsobené zneužitím odcizené karty nese držitel karty podle podmínek banky, která kartu vydala. [38]

- **Zneužití karty osobou blízkou –** velkou část podvodů dělají blízcí příbuzní, děti, přátelé a spolupracovníci (kteří znají PIN kód karty, případně i její další nutné individualizační údaje). Motivem nemusí být pouze majetkový prospěch, ale i „řešení“ různých vzájemných neshod. [38]
- **Horké krádeže platebních karet –** jedná se o krádež platební karty, kterou ještě oprávněný držitel nezaregistroval. Tyto krádeže vedou často k odčerpání značných finančních částek z účtu držitele platební karty, a to zvláště v případech, kdy má pachatel současně k dispozici i nějaký osobní doklad poškozené osoby (občanský průkaz, cestovní pas). Riziko neoprávněného výběru vyšších finančních částek nebo finančních transakcí se zvyšuje se speciálním charakterem platebních karet (stříbrné či diamantové platební karty). Odcizené platební karty lze dokonce v některých případech i dodatečně zpeněžit jejich odevzdáním u emitenta a inkasovat částku za jejich navrácení jako karet „nalezených“.[38]
- **Krádež – navrácení –** odcizená platební karta je oprávněnému držitel následně vrácena, ovšem za podmínek, kdy oprávněný držitel o krádeži neví, a tedy ani netuší, že s jeho platební kartou bylo nelegálně nakládáno, a proto neuskutečnil kroky k jejímu zablokování. V období, kdy platební kartu nemá oprávněný držitel k dispozici, dochází k nelegálním výběrům z účtu, překopírování elektronických údajů (tzv. skimming) nebo k opsání identifikačních údajů. Poškozená osoba se o nedovoleném použití platební karty mnohdy dozví až ze zaslaného výpisu z účtu a případné následné reklamace bývají značně problematické. [38]

---

[38] SADOVSKÝ, Dalibor; SUCHÁNEK, Jaroslav. Platební karty a možnosti jejich zneužití. Kriminalistika [online]. 2004, č. 1 [cit. 9. února 2011]. Dostupné z: <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0401/suchanek_info.html>.

- **Podvodné žádosti –** jejich podstatou je skutečnost, že pachatel k žádosti o vydání platební karty předloží pozměněné nebo padělané osobní doklady. V případě úspěchu, je vydána platební karta neexistující osobě, jejíž následná identifikace je nemožná nebo velmi obtížná. [39]
- **Zneužití nedoručené platební karty –** nastává v případech, kdy emitent platební karty zasílá platební kartu držiteli poštovním stykem. V tomto případě zasílá emitent odděleně platební kartu a příslušný PIN kód. Protože platební karta nemá podepsaný podpisový proužek, naskýtá se pachateli možnost proužek podepsat a kartu zneužít. V současnosti je preferováno osobní převzetí platební karty na příslušném výdejním místě, případně je požadována telefonická zpětná kontrola o úspěšném poštovním předání platební karty včetně uvedení hesla, které bylo mezi emitentem a držitelem karty domluveno při sjednání smlouvy. V opačném případě je platební karta blokována a nezpůsobila k provádění příslušných transakcí. [39]
- **Přepsané prodejní doklady –** jedná se zneužití platebních karet ze strany obchodníků. Tento způsob lze uskutečnit pouze s embosovanými platebními kartami, pokud jsou jejich údaje snímány zařízením zvaným imprinter (slangově „žehličkou“). Imprinter je mechanické zařízení, které vytvoří otisk (kopii) platební karty na papírový předtisk a zároveň na něm uvede identifikaci obchodního místa. Z této provedené transakce se vyhotovuje ve třech vyhotoveních pokladní doklad, který po autorizaci podpisem je v jednom výtisku dán kupujícímu, druhý si pro své vyúčtování ponechává obchodník a třetí výtisk je zaslán zúčtovacímu bankovnímu domu k povedení příslušné finanční transakce. Obchodník může nelegálně upravit výši zaplacené částky na dokladu, který si ponechá pro vyúčtování, i na dokladu, který zasílá k zúčtování příslušnému bankovnímu domu. V případech problémů a reklamací, pokud plátce již nemá kopii dokladu k dispozici (např. po její ztrátě) se dostává do situace důkazní nouze a jeho, byť oprávněné nároky prosu problematizovány. [39]

---

[39] SADOVSKÝ, Dalibor; SUCHÁNEK, Jaroslav. Platební karty a možnosti jejich zneužití. Kriminalistika [online]. 2004, č. 1 [cit. 9. února 2011]. Dostupné z: <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0401/suchanek_info.html>.

- **Vícenásobné otisky –** ze strany obchodníku přicházení v úvahu i další případy trestné činnosti s platebními kartami. Nejvýznamnější jsou tzv. vícenásobné otisky. Pachatel trestné činnosti (obchodník) opakovaně neoprávněně „přežehlí“, přesněji zkopíruje údaje z platební karty na předtisk účtenky – to mu nechtěně umožní oprávněný držitel platební karty např. tím, že platební kartu ztratí ze svého dohledu (bez fyzické kontroly ji např. předá účtujícímu číšníkovi). Následně po úpravě finanční částky na některé kopii pachatel doplní dalším „žehlením“ identifikační údaje o obchodním místě, účtenku doplní „pravým“ podpisem držitele a předá ji k proplacení příslušnému bankovnímu domu. [40]

3.2 Padělání platebních karet

3.2.1 Skimming

Závažným druhem trestné činnosti s platebními kartami je tzv. skimming. Jedná se o způsob páchání trestné činnosti, který vede k vytvoření padělku platební karty. V současnosti je považován za jednu z nejnebezpečnějších i nejzávažnějších forem páchaní trestné činnosti s platebními kartami. [40]

„Obecně lze skimming definovat tak, že se jedná o přípravu a výrobu různých zařízení, které pachatelé nasazují na bankomaty, pokladní terminály v obchodech a jiných místech nebo na výdejný automaty na výdej pohonných hmot, jízdenek atd., kde lze k platbě použít platební karty s tím, že cílem pachatele je nejprve nezákonné získání dat z magnetického proužku nebo čipu karty a zadávaného kódu PIN, následně výroba padělku platební karty (formou úpravy pravé nebo použitím jakékoliv klubové, věrnostní, telefonní a jiné karty) a v konečné fázi použití padělku karty k výběrům peněz z bankomatů nebo platbě kartou za zboží na pokladním terminálu či výdejním automatu nebo zneužití dat k transakcím na internetu. Výsledným efektem skimmingu je však vždy nezákonné odčerpání finančních prostředků z účtu držitele platební karty.“[41]

Skimming se skládá z několika dílčích kroků, které na sebe logicky navazují.

---

[40] SADOVSKÝ, Dalibor; SUCHÁNEK, Jaroslav. Platební karty a možnosti jejich zneužití. Kriminalistika [online]. 2004, č. 1 [cit. 9. února 2011]. Dostupné z: <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0401/suchanek_info.html>.

[41] Internetové stránky Karty-peníze. Dostupné z: <http://www.karty-penize.webgarden.name/menu/skimming>. [cit. 18. února 2011]

V první fázi dochází k nelegálnímu zkopírování záznamu z magnetického proužku platební karty, včetně zkopírování zakódovaných údajů. K tomu jsou využívána miniaturní zařízení, která lze mnohdy skrýt v ruce (při platbách v obchodech či v restauracích) nebo jsou ilegální součástí vstupních dveří, které umožňují přístup k bankomatům (zájemce o služby bankomatu může vstupní dveře otevřít pouze uplatněním platební karty – jejím „protažením" čtecím zařízením). Paměťová kapacita uvedených zařízení umožňuje záznam 100 až 200 kompletních údajů z platebních karet. K tomuto zkopírování dochází v případech, kdy držitel platební karty nemá přehled o jejím pohybu nebo nemá bez použití platební karty přístup k příslušnému bankovnímu terminálu. Vlastní operace trvá řádově sekundy.[42]

V druhé fázi provede pachatel zkopírování nelegálně získaných údajů pomocí počítače a příslušného softwaru na pevný disk počítače. [42]

V konečné fázi „nahraje" pachatel údaje z počítače na bianco vytvořenou platební kartu opatřenou příslušným magnetickým proužkem. Může se jednat o „bílý plast", ale i o platební karty (nejčastěji odcizené nebo nalezené), které vykazují všechny atributy platné platební karty, z níž byly původní elektronické údaje odstraněny a nahrazeny údaji novými.[42]

Skimming je zákeřným a skrytým způsobem trestné činnosti, protože k odcizení dat z platební karty dochází bez toho, aby se o tom poškozený vůbec dozvěděl, a o odčerpání finančních prostředků se dozví často až z upozornění banky o blokaci karty či její výměně nebo z výpisů z karty. K nezákonným výběrům dochází bezprostředně po zcizení dat, ale také i po delším časovém úseku, řádově i roků. Skimmingem se zabývá organizovaná skupina pachatelů (převážně se jedná o gangy založené na národnostním principu – známé jako rumunské a bulharské), většinou propojená na základě rodinných vztahů nebo místa bydliště. [43]

Nejznámějším a nejrozšířenějším způsobem skimmingu na celém světě je získávání dat z platebních karet a PIN kódu na bankomatech. Pachatelé nasadí na bankomat zařízení na skimmování dat (jeden nástavec je nasazen na vstupní štěrbinu bankomatu pro vsunutí platební karty a obsahuje elektroniku pro záznam dat z magnetického proužku karty a druhý

---

[42] SADOVSKÝ, Dalibor; SUCHÁNEK, Jaroslav. Platební karty a možnosti jejich zneužití. Kriminalistika [online]. 2004, č. 1 [cit. 9. února 2011]. Dostupné z: <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0401/suchanek_info.html>.

[43] Internetové stránky Karty-peníze. Dostupné z: <http://www.karty-penize.webgarden.name/menu/skimming>. [cit. 18. února 2011]

nástavec, který obsahuje elektroniku, často to bývá mobilní telefon, pak zaznamenává na videosoubor zadávaný PIN kód). Tyto zařízení zde na určitou časovou dobu nechají. Tato doba se liší podle toho, zda získaná data lze přenášet do notebooku pachatelů bezdrátově (Bluetooth, WiFi) nebo je musí z bankomatu sundat a data do notebooku stáhnout drátovým připojením. Pokud občan v této době použije bankomat k výběru peněz, tak tyto peníze sice bez problému vybere, ale současně pachatelé získají potřebná data.[44]

V příloze č. 1 – Skimmovací nástavce na bankomatech, jsou zobrazeny fotografie bankomatů s a bez skimovacích zařízení.

Dalším způsobem skimmingu je získávání dat z platebních karet a PIN kódu na pokladních terminálech ve velkoobchodech, obchodních řetězcích, hotelech, čerpacích stanicích apod., kde se pachatelé snaží různými způsoby vyměnit originální pokladní terminála za upravené a způsobilé zaznamenat data z magnetického proužku karty i zadávaný PIN kód. Tyto zde opět ponechají, často i jeden měsíc a poté je odnesou. Většinou výměnu terminálu provedou maskovaní za servisní techniky nebo se skrytě do objektu vloupají, např. střechou. Tento způsob skimmingu zatím v České republice nebyl zjištěn. [44]

Příloha č. 2 – Upravené pokladní terminály, obsahuje dva obrázky, na kterých jsou upravené pokladní terminály.

Méně známým způsobem skimmingu v ČR, ale rozšířeným např. v USA, Kanadě nebo Velké Británii je získávání dat z platebních karet a kódů PIN na výdejních stojanech (čerpací stanice, prodej jízdenek MHD a metra). Tyto automaty velmi často používají stejné otvory pro vsunutí platebních karet i klávesnice k zadávaní PIN kódů a pachatelé na automaty nasazují podobné nástavce jako na bankomaty. [44]

Příloha č. 3 – Skimmovací zařízení čerpacích stanic. Na obrázku č. 1 je skimmovací zařízení čerpací stanice a obrázek č. 2 zobrazuje detail skimmovacího zařízení čerpací stanice.

Specifickým způsobem skimmingu je získání dat z magnetického proužku nebo čipu platební karty i zadávaného PIN kód hackery, prostřednictvím internetu nebo stažením dat pomocí podplacené osoby z počítače, např. organizace zabývající se zpracováním platebních transakcí v určitém teritoriu. Tento způsobe je velmi nebezpečný, protože se zde pachatelům

---

[44] Internetové stránky Karty-peníze. Dostupné z:
<http://www.karty-penize.webgarden.name/menu/skimming>. [cit. 18. února 2011]

podaří rychle a relativně bezpečně získat obrovské množství dat z platebních karet najednou. [44]

3.3 Podvody prostřednictvím bankomatu

Pachatelé trestné činnosti využívají k jejímu uskutečňování také provoz bankomatů. Bankomat je přístroj, který slouží k vybírání hotovosti pomocí platební karty. Je vybaven klientskou a operátorskou zónou. V klientské části, neboli také v tzv. obslužné zóně se nachází monitor, klávesnice, čtečka karet, výplatní slot a tiskárna účtenek. V operátorské části, která je určena pouze obsluze bankomatu, je umístěn trezor, v němž se nachází výplatní a kódovací modu. V této části je také umístěn řídící počítat, žurnálová tiskárna, operátorský monitor a klávesnice. Bankomaty bývají zpravidla víceúčelové, tzn., že držitel platební karty má možnost nejen vybírat po zadání PIN kódu hotovost, ale i zjistit, jaký má zůstatek na svém účtu, popř. si může dobýt svůj mobilní telefon. Bankomaty jsou konstruovány tak, aby se zamezilo jejich poškození, navíc z bezpečnostních důvodů bývají ukotveny speciálními úchyty k podlaze. Některé instituce bankomaty vybavují i kamerovým systémem, který monitoruje nedovolenou manipulaci s bankomatem.[45]

Za bezkontaktní způsob získávání utajovaných informací o PIN kódu lze považovat sledování držitele platební karty a jeho zadávání uvedeného kódu. Za kvalifikovanější způsoby lze považovat instalaci utajených miniaturních televizních kamer, které zaznamenávají pohyb prstů a stisk jednotlivých kláves bankomatu při zadávání PIN kódu. [45]

Bankomaty jsou chráněné před napadáním pachateli trestných činů i mechanickými zabezpečovacími prvky. Protože bankomaty obsahují značné finanční částky v hotovosti, je nezbytné jejich zabezpečení před odcizením či násilným otevřením. Toto se řeší vysokou hmotností – většinou 700 – 1 000 kg, mechanickou odolností větších ploch i pevným připojením ke stavebnímu podkladu, které je přístupné až po překonání trezorové části. Běžně je využívána elektronická signalizace, která zprostředkovává na příslušné pracoviště informaci o neoprávněné manipulaci s bankomatem (policejní útvar nebo pult centralizované ochrany bezpečnostních služeb). [45]

---

[45] SADOVSKÝ, Dalibor; SUCHÁNEK, Jaroslav. Platební karty a možnosti jejich zneužití. Kriminalistika [online]. 2004, č. 1 [cit. 9. února 2011]. Dostupné z: <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0401/suchanek_info.html>.

Bankomaty mohou také fungovat i jako prostředek ke zneužití platebních karet. Jedná se o tyto způsoby zneužití:

3.3.1 Aplikace falešného (neautentického) předního krytu bankomatu

Spočívá v tom, že se do prostoru před originální bankomatový kryt umístí duplikát. Po zasunutí platební karty do snímače se karta zachytí v prostoru mezi pravým a falešným krytem. Pachatel ji následně vyjme a odcizí. [46]

3.3.2 Lisabonská smyčka

Spočívá v zasunutí a fixování vhodně zastřiženého ústřižku do štěrbiny snímače platební karty v bankomatu. Přítomnost ústřižku není zevně z venku zpravidla běžně patrná. Při zpětném pohybu platební karty po provedené finanční transakci (ještě před vydáním finanční hotovosti z bankomatu) se platební karta „zasekne“ a nelze ji z bankomatu vyjmout. Pachatel, který bývá většinou poblíž, ujistí držitele o tom, že se mu to před chvíli stalo také a že by bylo vhodné, aby zopakoval zadání PIN kódu (který si zapamatuje). Někteří pachatelé uvádění, že postačí k navrácení platební karty zadání PIN kódu třikrát za sebou (tím má pachatel větší pravděpodobnost, že si PIN kód zapamatuje). Pokud ani po této operaci nedojde k vydání platební karty, pachatel sdělí, že náhodou zná telefonní číslo na provozovatele bankomatu (které je ve skutečnosti falešné) a o neuskutečněné transakci provozovatele bankomatu informoval. Telefonickým rozhovorem si spolupachatel na falešném telefonním čísle opětovně ověří kromě jiného i PIN kód. Po odchodu držitele platební karty ji z bankomatu pachatel pomocí pinzety vyjme, vyjme také použitou fólii a uskuteční nelegální výběr hotovost, jelikož zná PIN kód. Variant uvedeného způsobu páchání trestné činnosti je více, hovoří se o využití tzv. „lisabonské smyčky“. Stejný způsob páchání trestné činnosti je ve Spolkové republice Německo označován jako „alžírská smyčka“. [46]

Příloha č. 4 – Lisabonská smyčka obsahuje 3 obrázky, na kterých je vyobrazena Lisabonská smyčka.

---

[46] SADOVSKÝ, Dalibor; SUCHÁNEK, Jaroslav. Platební karty a možnosti jejich zneužití. Kriminalistika [online]. 2004, č. 1 [cit. 9. února 2011]. Dostupné z: <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0401/suchanek_info.html>.

3.3.3 Hradecká lišta

Dalším způsobem, který se v České republice poprvé objevil v roce 2008, je tzv. Hradecká lišta. Jedná se o falešnou zádržnou lištu (zjištěná poprvé na bankomatech v Hradci Králové), nebo falešný nástavec překrývající otvor pro výdej peněz na bankomatu. Na liště nebo nástavci je z vnitřní strany nalepena oboustranná lepicí páska. Jestliže občan přijde k bankomatu, který obsahuje takovéto zařízení, většinou si ničeho nevšimne a vloží kartu do vstupního otvoru, zadá potřebné údaje pro výběr peněz, karta mu vyjede zpět, ale bankomat mu nevydá žádné peníze. Ty jsou přilepeny na vnitřní straně zádržné lišty nebo nástavce a ani nemohou vyjet ven. Pachatelé si pak počkají, až občan odejde závadu reklamovat, lištu odtrhnou a peníze si vezmou. Lištu nebo nástavec pak pachatelé znovu nasadí a čekají na dalšího občana. Často tak přecházejí mezi několika poblíž umístěnými bankomaty. Řada případů nasazených tzv. Hradeckých lišt se vyskytla i v roce 2009 a 2010 v Praze. [47]

V příloze č. 5 – Hradecká lišta jsou dva obrázky zobrazující tuto lištu.

3.3.4 Instalace falešných bankomatů

Pro uplatnění tohoto trestného činu je třeba mít značné odborné znalosti i finanční prostředky. Pachatelé nainstalují plně funkční bankomat na vhodné frekventované místo. Bankomat je opatřen běžnými údaji, jsou na něm loga emitenta a další údaje a jako celek budí naprosto věrohodný dojem. Po určitou dobu uskutečňuje také požadované služby (vydává peněžní částky v hotovosti). Ve skutečnosti však překopírován údaje z platebních karet, které ukládá do paměti. Takto získané údaje následně pachatelé zneužívají pro páchání trestné činnosti. [48]

3.3.5 Podvodné manipulace s bankovkami při výdeji hotovosti z bankomatu

Tato trestná činnost je možná pouze v případech, kdy jsou bankomaty vybaveny funkcí, která po určité době (např. sekund) provede zpětvzetí bankovek, které nebyly odebrány

---

[47] Internetové stránky Karty-peníze.

Dostupné z: <http://www.karty-penize.webgarden.name/menu/skimming>. [cit. 18. února 2011]

[48] SADOVSKÝ, Dalibor; SUCHÁNEK, Jaroslav. Platební karty a možnosti jejich zneužití. Kriminalistika [online]. 2004, č. 1 [cit. 9. února 2011]. Dostupné z: <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0401/suchanek_info.html>.

z výdejové štěrbiny. Bankomat provedenou transakci zruší a z účtu držitele platební karty není odečtena příslušná částka. Pokud pachatel z vydávaného svazku bankovek několik odejme, bankomat tuto skutečnost nezaregistruje a do jeho zásobníku se vrátí menší finanční částka. [48]

3.3.6 Zneužití postavení odpovědného pracovníka

Jedná se o trestnou činnost, která je prováděná při doplňování hotovosti v bankomatech. Zjištěný deficit je pachatelem různými způsoby vysvětlován. Jedná se o trestnou činnost, jejíž podstatou není činnost spojená se zneužíváním platebních karet. [48]

3.4 Podvody bez přítomnosti platební karty

Jedná se o trestnou činnost, při které pachatelé zneužívají možností prodeje, koupě či poskytnutí nejrůznějších služeb s využitím různých komunikačních prostředků (telefonu, faxu, internetu, apod.). Pro uskutečnění transakce vyžadují poskytnutí údajů z platebních karet (číslo platební karty, PIN kód, dobu její platnosti, typ karty). Adresy prodejců nebo poskytovatelů služeb bávají smyšlené a případné reklamace nebo možné právní řešení problémů bývá velmi problematické. [48]

3.5 Zneužití internetového bankovnictví

3.5.1 Odposlouchávání klávesnice

Existují programy, které umí odečítat hesla a jiné identifikační údaje z klávesnice. Klient zadává údaje na klávesnici a tento program rozezná podle úhozů na klávesnici, které klávesy byly stisknuty. Hacker si poté tyto údaje dokáže snadno zjistit.

Proto některé banky, jako např. Česká spořitelna používá přímo nastavenou klávesnici na přihlašovací stránce. Klient své údaje zadává pomocí myší a tudíž nemůže dojít k odečtení údajů z klávesnice.

Obrázek 3.1 - Internetbanking České spořitelny

Zdroj: Internetové stránky České spořitelny. Dostupné z:
< https://www.servis24.cz/ebanking-s24/dispatcher>. [cit. 15. února 2011]

3.5.2 Phisihing

O původu slova phishing se tvrdí dvě teorie. Jedna tvrdí, že vzniklo úpravou slova fishing – rybaření, kdy „f“ bylo změněno za dvojici písmen „ph“. Druhá předpokládá, že jde o zkratku: „password harvestin fishing – sběr hesel rybařením. Phishing se česky překládá jako „rhybaření“. Postup podvodníků připomíná rybaření, jelikož rozešlou e-maily na mnoho náhodných adres (jako když rybáři hodí sítě do vody) a čekají, kdo se nachytá a sdělí důvěrné informace. [49]

Tato podvodná technika útočí na důvěřivost lidského prvku, dochází při ní k zneužití emailové pošty s cílem získání identifikačních údajů. Riziko spočívá v tom, že do e-mailového formuláře vyplníte číslo své platební karty s dalšími osobními údaji. E-mail,který se jeví, že byl doručen bankovní institucí je však podvodný a pokud dojde k zadání těchto citlivých dat, může dojít v krátkém časovém sledu k výrobě padělku platební karty a následně k jejímu zneužití. Během několika minut může dojít k výběru z bankomatu v zahraničí. [50]

---

[49] Internetové stránky Hoax. Dostupné z: <http://www.hoax.cz/phishing/co-je-to-phishing>.
[cit. 18. února 2011]

[50] Internetové stránky Sdružení českých spotřebitelů.
Dostupné z: <http://www.prevencepodvodu.cz/platebni-prostredky/bezhotovostni-platby/bankomat-atm.php>. [cit. 9. února 2011]

Nejčastěji se snaží vylákat údaje k platebním kartám včetně PIN kódu nebo různé přihlašovací údaje. Nemusí jít jen o bankovní účty, ale tako účty ostatních organizací, kde dochází k manipulaci s penězi nebo je možné jakýmkoliv způsobem zneužít jejich služeb. Např. PayPal, eBay, Skype, Google. [51]

Základní znaky phishingového emailu: [51]

- Snaží se vyvolat doje, že byl odeslán organizací, z jejichž klientů se snaží vylákat důvěrné informace. Tohoto se snaží docílit grafickou podobou e-mailu a zfalšováním adresy odesílatele.
- Text může vypadat jako informace o neprovedení platby, výzva k aktualizaci bezpečnostních údajů, oznámení o dočasném zablokování účtu či platební karty, výzkum klientské spokojenosti nebo jako elektronický bulletin pro klienty.
- V textu zprávy je link, který na první pohled většinou vypadá, že směřuje na stránky banky. Ve skutečnosti ale odkazuje na jiné místo, kde jsou umístěny podvodné stránky.
- Jestliže klient klikne na odkaz v e-mailu, dostane se na falešné stránky podvodníků, které jsou vytvořeny ve stejném stylu, jako originální stránky banky. Na podvodných stranách je připraven formulář, kde jsou požadovány důvěrné informace – čísla účtu, kódy k internetovému bankovnictví, PIN k platební kartě, přihlašovací údaje ke službám apod.

Phishing není žádnou novinkou, první záznamy jsou z poloviny 90. let minulého století. Masově se rozšířil počátkem tohoto století. Jeden z prvních odchycených e-mailů byl z května 2004 u CityBank. Dokonalejší pokus je z února 2005, kdy se panovníci snaží maskovat adresu v e-mailu a zobrazovanou adresu v internetovém prohlížeči překrýt podstrčeným obrázkem. Ze stejného měsíce pochází další zajímavý trik, kdy se podvodníci snaží svoji oběť přesvědčit, že e-mailu v odkazu směřuje do správné domény. [52]

V březnu 2006 byl zaznamenán první český útok na klienty CityBank. U tohoto podvodu bylo využito nového triku, tzv. smart redirection, což se dá přeložit jako „chytré

---

[51] [Internetové stránky Hoax. Dostupné z: <http://www.hoax.cz/phishing/co-je-to-phishing>.
[cit. 18. února 2011]

[52] Internetové stránky Hoax. Dostupné z: <http://www.hoax.cz/phishing/co-je-to-phishing>.
[cit. 18. února 2011]

přesměrování“. Odkaz v podvodném e-mailu odkazuje na místo, kde je umístěn „inteligentní směrovač“, který oběť přesměruje na některý z mnoha nastražených podvodních webů.

V příloze č. 6 je zobrazen první phishingový útok v České republice na klienty CityBank. Příloha obsahuje podvodný e-mail a podvodné okno.

V říjnu 2006 byl proveden první útok na klienty České spořitelny. Až na pár výjimek byl napsán poměrně dobře česky. Tyto skutečnosti zobrazuje příloha č. 7. Je zde vzhled podvodného e-mailu a vzhled podvržené stránky.

Od počátku roku 2008 začaly masivní útoky na klienty České spořitelny, které se až do Velikonoc stupňovaly. Nejdříve to byly úsměvné pokusy s neumělou češtinou. S největší pravděpodobností se jednalo o strojové překlady a oslovení. „Drahoušek zákazník“ se stalo oblíbeným sloganem. Tento podvodný e-mail je zobrazen v příloze č. 8, konkrétně obrázek č. 1 – Drahoušek zákazník. Další pokusy varovaly před neprovedenou transakcí nebo slibovali odměnu za vyplnění dotazníku. Taktéž se nachází v příloze č. 8, obrázky 2 a 3.Všechny tyto podvodné e-maily byly psány buď anglicky, nebo nepovedenou češtinou. Zlom nastal až ve chvíli, kdy podvodníci použili velmi jednoduchý trik. Text okopírovali přímo ze stránek České spořitelny. Zneužily aktualitu, která varuje před podvodnými e-maily. V textu sice varovali před sebou samými, ale nechyběl odkaz na „verifikaci“ svého účtu, který směřoval na podvodné stránky. Tento podvodný e-mail obsahuje příloha č. 8, obrázek č. 4.

3.5.3 Pharming

Pharming je podvodná technika používaný na internetu k získání citlivých údajů od obětí útoku. Někdy je překládán do češtiny jako farmaření. Funguje tak, že se klient přihlásí na normální stránku banky, vydá své přístupové kódy k účtům a nemá možnost si všimnout, že se jedná o podvodnou stránku. [53]

První podoba pharmingu je sice efektivní, ale pro podvodníka, který chce jejím prostřednictvím získat citlivé údaje, značně obtížná. Spočívá v tom, že klient zadá ve svém internetovém prohlížeči nějakou adresu. Nedojde ale k jejímu překladu na správnou adresu, ale na adresu, kterou zadali podvodníci. Spojení s bankou je přesměrováno na jiný kanál, jehož www stránky, které připravili podvodníci, jsou velice podobné oficiálním stránkám

[53] Internetové stránky Trojanhelp. Dostupné z: <http://trojanhelp.wz.cz/pharming.htm>. [cit. 7. dubna 2011]

klientovy banky. Při přihlášení klienta ke komunikaci s bankou získají podvodníci citlivé údaje a bude následovat odčerpání finančních prostředků z klientova účtu. [54]

Druhá podoba pharmingu je pro podvodníka jednodušší, tudíž i více používána. Spočívá v tom, že podvodníci napadají jednotlivé počítače. Pharming se do klientova počítače může dostat jako trojský kůň, který je poslán v příloze e-mailu, může být stažen apod. [54]

Tento podvod může být spáchán několika způsoby: [55]

- název domény může být vytvořen velmi podobným názvem k názvu webové stránky, aby došlo ke zmatení uživatele
- může být vytvořeno falešné propojení z jiných webových stránek, které vede na falešnou webovou stránku
- toto může být kombinováno s phisihingem přidáním falešného propojení na email

Zločinci se snaží získat osobní informace pro přístup k bankovním účtům, ukrást údaje totožnosti nebo spáchat jiný podvod jménem uživatele. Pharming je případem měnící se doby, útoky nejsou zaměřeny pouze na ovlivnění uživatelů, ale na vytváření finančních zisků.[55]

3.5.4 Spoofing

Tato technika není v České republice dosud rozšířena. Spoofing znamená doslova napálit, převézt, vodit na nos. Patří mezi nejnebezpečnější zbraně těch, kteří chtějí neoprávněně proniknout do cizích sítí. Podstata podvodu spočívá v tom, že se určitý uzel sítě vydává za „někoho jiného“. V důsledku tzv. „osahávání“ serverů nebo lokálních sítí mohou být za určitých podmínek zjištěna citlivá data, která mohou být následně zneužita. [54]

Tato metoda podvodu se zaměřuje na metodu krádeže identity. Spoofing se používá pro mnoho různých účelů. Primárně pro získání informací o uživateli, např. jaké navštěvuje stránky, hesla, soukromé informace o uživateli apod.[56]

---

[54] Internetové stránky Sdružení českých spotřebitelů. Dostupné z: <http://www.prevencepodvodu.cz/platebni-prostredky/bezhotovostni-platby/bankomat-atm.php>. [cit. 9. února 2011]

[55] Internetové stránky Konzument. Dostupné z: <http://www.konzument.cz/publikace/soubory/pruvodce_spotrebitele/EvropDokumentace_podvody.pdf>. [cit. 23. února 2011]

3.5.5 Trashing

Jedná se o další z moderních způsobů podvodů. Je také založený na zjištění citlivých dat. Název je odvozen od anglického trash (koš). Jde v podstatě o „vybírání odpadků“, z nichž lze zjistit řadu zajímavých informací. Výjimkou nejsou přístupová hesla, zdrojové kódů apod. [57]

3.5.6 Smishing

Je to varianta phisnihgu, ve které jsou k získání informací použity SMS zprávy. Uživatel obdrží SMS zprávu, která ho vláká na telefonní čísla nebo provedení bankovních převodů za různými účely. Odesílatel zprávy je také odesílatel spamů, která se snaží převzít identitu známého, kolegy nebo společnosti ze seznamu kontaktů. Oběť obdrží SMS zprávu říkající, že si předplatila on-line datovací službu, nebo jinou službu, a že tato služba bude připsána k účtu za telefon. Zpráva také nabízí spojení k webovým stránkám z telefonu pro přerušení služby. Mnoho lidí provedou propojení, aby odvolali službu. Oběti se poté dostanou tam, kde chce podvodník a může být vystaven nedobrovolnému stahování trojského koně nebo jiného druhu podvodného programu. [56]

Jinou metodou je zaslání SMS zprávy, říkající, že banka provedla velkou platbu z účtu oběti, na kterou neexistují dostatečné prostředky. Při zavolání je oběť konfrontována sérii zaznamenaných zpráv, které ji vedou k tomu, aby uvedla podrobnosti bankovního účtu. [56]

3.5.7 Vishing

Způsob, který je podobný phishingu, ale s rozdílem, že místo zaslání emailu jsou uskutečňovány telefonní hovory, které žádají čísla kreditních karet, PIN kódů apod. Zločinec konfiguruje „válečné vytáčení“ (vytáčení série telefonních čísel, aby byla nalezena ta, která jsou připojena k modemu, aby umožnila připojení k jinému počítači) v určité oblasti. [56]

---

[56] Internetové stránky Konzument. Dostupné z:

<http://www.konzument.cz/publikace/soubory/pruvodce_spotrebitele/EvropDokumentace_podvody.pdf>. [cit. 23. února 2011]

[57] Internetové stránky Sdružení českých spotřebitelů. Dostupné z:

<http://www.prevencepodvodu.cz/platebni-prostredky/bezhotovostni-platby/bankomat-atm.php>.

[cit. 9. února 2011]

- Když je volání reagováno, ozve se alarm a upozorňuje „spotřebitele“, že jeho karta je podvodně použita a že by měl okamžitě zavolat následující číslo. Číslo je falešné bezplatné telefonní číslo „banky“.
- Když oběť zavolá na číslo banky, odpoví jí počítač, který sdělí klientovi, že jeho účet musí být ověřen a že musí uvést 16 číslic své kreditní karty.
- Když oběť uvede číslo své kreditní karty, podvodník má všechny informace potřebné k provedení podvodných transakcí s kartou.
- Hovor je často také použit k získání PIN kódů, dat platností, čísel účtů a jiných informací.

3.5.8 Trojský kůň

Trojské koně jsou programy, které jsou schopny zůstat v počítačích, aby umožnily přístup vnějším uživatelů, prostřednictvím místní sítě nebo internetu s cílem shromažďovat informace nebo ovládat na dálku hostující stroj. Trojský kůň sám není virus, i když může být šířen a fungovat jako virus. Je obvykle používán pro tajné získávání informací za použití metody pro instalaci softwaru, který umožní na dálku přístup ke sledování toho, co uživatel počítače dělá a např. zaznamenává klávesnicové úhozy, aby získal hesla nebo jiné informace pro spáchání podvodu. Zjištěné informace pak předává svým tvůrcům.[58]

3.5.9 Malware

Jedná se o všeobecné označení pro škodlivé programy. Napadené počítače mohou sloužit ke sběru adres, šíření spamu, včetně phishingových e-mailů a šíření dalšího malware. [58]

3.5.10 Nigerijské dopisy

Jedná se o řetězový e-mail, který požaduje pomoc pro nemocného, opuštěný zvířata, nebo jakékoliv jiné způsoby zkonstruované pro apelování na smysly čtenáře. Ale tyto e-maily nejsou ničím jiným než formou podvodu. [59]

---

[58] Internetové stránky Konzument. Dostupné z:

<http://www.konzument.cz/publikace/soubory/pruvodce_spotrebitele/EvropDokumentace_podvody.pdf>. [cit. 23. února 2011]

[59] Internetové stránky Konzument. Dostupné z:

<http://www.konzument.cz/publikace/soubory/pruvodce_spotrebitele/EvropDokumentace_podvody.pdf>. [cit. 23. února 2011]

Tyto dopisy mají formu e-mailu informujícího příjemce, že vyhrál loterii nebo slosování nebo žádající o pomoc při vyhnutí se dani z příjmu za značnou odměnu. Ve skutečnosti se pokouší podvést uživatele, která je pak požádán o zaslání určitého množství peněz pro zaplacení celních poplatků, spotřebních daní, odměny úředníkům apod., aby mohl obdržet odměnu, která se však nikdy neuskuteční.[60]

Jedná se o jednu z nejškodlivějších podvodných praktik pro oběti. Je velmi obtížné získat zpět peníze, jelikož jsou obvykle zasílány do zemí s malým nebo, nebo vůbec, právním zabezpečením, kde peníze velmi rychle zmizí. [60]

3.6 Další útoky

Mezi další útoky se řadí Cross-Site Scripting, Cross-Site Forgery a Clicjacking. Tyto formy útoku nebyly zatím ještě použity ke zneužití internetového bankovnictví, ale je jen otázku času, kdy k tomu dojde.

3.6.1 Cross-Site Scripting

Cross-Site Scripting, zkráceně XSS, je metoda narušení WWW stráněk využitím bezpečnostních chyt ve skriptech. Útočník díky těmto chybám v zabezpečení webové aplikace dokáže do stránek podstrčit svůj vlastní javascriptový kód. Toto může využít jak k poškození vzhledu stránky, tak i k jejímu znefunkčnění anebo dokonce získávání citlivých údajů návštěvníků stráněk, obcházení bezpečnostních prvků aplikace a phishingu. [61]

3.6.2 Cross-Site Request Forgery

CSRF nebo také XSFR je typ útoku na webovou aplikaci nebo službu pracující na bázi neočekávaného požadavku pro vykování určité akce v této aplikace, který ale pochází z nelegitimního zdroje. Většinou se jedná o útok směřující k získání přístupu do aplikace.[62]

Podstata útoku spočívá v tom, že uživatele přiměje navštívit stránku napadené aplikace, která provádí nějakou akci, aniž by o tom uživatel věděl. Útok může být snadno veden proti

---

[60] Internetové stránky Konzument. Dostupné z:
<http://www.konzument.cz/publikace/soubory/pruvodce_spotrebitele/EvropDokumentace_podvody.pdf>. [cit. 23. února 2011]

[61] Internetové stránky Wikipedia. Dostupné z: <http://cs.wikipedia.org/wiki/Cross-site_scripting>.
[cit. 21. února 2011]

[62] Internetové stránky Wikipedia Dostupné z:
<http://cs.wikipedia.org/wiki/Cross-site_request_forgery>.[cit. 21. února 2011]

aplikacím, do kterých se útočník může sám přihlásit a tím zjistit jejich strukturu nebo které mají přístupový zdrojový kód. [63]

3.6.3 Clickjacking

Jedná se o způsob útoku na uživatele webových stránek, při kterém uživatel nějakou činností na zdánlivě neškodné stránce (např. kliknutím na tlačítko či obrázek) spustí akci, kterou nepředpokládal. Stránka využívající clickjacking má na pozadní neškodný obsah (např. vtipné obrázky) a vedle nich odkaz, který o sobě tvrdí, že vede na další stránku obrázků. Dále je však do stránky vložen rám se zcela jinou stránkou a ten je zobrazen přes obsah na pozadí, ale se zapnutou průhledností, tudíž o něm uživatel neví. Když se následně uživatel pokusí kliknout na odkaz, který má vést na další stránku, ve skutečnosti kliká na neviditelnou stránku. Tím může na cílové stránce provést prakticky libovolnou akci, aniž by o tom věděl a souhlasil. Nová stránka může být např. zabezpečený web, na který se uživatel musí přihlašovat heslem. Stačí, aby se někdy předtím na tento web přihlásil a server si stále jeho přihlášení pamatoval, pak se akce provede tak, jako by ji tento přihlášený uživatel provedl úmyslně. [64]

Pouze tři z českých bank jsou bezpečné proti tomuto útoku. Komerční banka, Citibank a mBank umožňují aplikovanou ochranu proti Clicjackingu. Zatímco si uživatel kliká třeba v rámci flashové hry, provádí se ve skutečnosti na pozadí klikání na originálním webu banky, kde se realizují akce, které by sám uživatel zcela jistě zamítl. Lze tak potvrdit platbu nebo umožnit útočníkovi skrze uživatele přístup k citlivým datům. Jedinou možnou ochranou je blokovat takovéto pokusy. Pouze Komerční banka, Citibank a mBank umožňují aplikovanou ochranu proti Clicjackingu.[65]

---

[63] Internetové stránky Php.vrana.cz. Dostupné z: <http://php.vrana.cz/cross-site-request-forgery.php>. [cit. 21. února 2011]

[64] Internetové stránky Wikipedia. Dostupné z: <http://cs.wikipedia.org/wiki/Clickjacking>. [cit. 21. února 2011]

[65] Internetové stránky Lupa.cz. Dostupné z: <http://www.lupa.cz/zpravicky/vetsina-ceskych-bank-neni-odolna-proti-clickjack>.[cit. 20. února 2011]

3.7 Statistika zneužití elektronického bankovnictví

Dříve, než si vymezíme prostředky k minimalizaci zneužití elektronického bankovnictví, tak je dobré se zmínit o statistice zneužití elektronického bankovnictví.

Tabulka 3.2 udává počet obžalovaných a odsouzených osob z trestného činu neoprávněné držení platební karty (§249b).

Tabulka 3.2 – Počet obžalovaných a odsouzených osob za trestný čin §249b v letech
2006 – 2009

	Trestný čin neoprávněné držení platební karty (§249b)			
	2006	**2007**	**2008**	**2009**
Obžalované osoby celkem	2045	2059	2035	1758
- ženy	344	394	350	288
- mladiství	212	201	206	217
Odsouzené osoby celkem	407	260	387	377
- ženy	99	85	105	87
- mladiství	22	22	24	23

Zdroj: Ročenky kriminality 2007 – 2010 Ministerstva spravedlnosti. Vlastní úprava.

Z tabulky je patrné, že počet obžalovaných a odsouzených osob se postupně snižuje. Do celkového počtu odsouzených osob nejsou zahrnuty případy, kdy došlo k uložení souhrnných trestů, byla povolena obnova řízení nebo podána stížnost pro porušení zákona.

Následující tabulka 3.3 zobrazuje počet nepodmíněných a podmíněných trestů za trestný čin neoprávněného držení platební karty.

Tabulka 3.3 – Podmíněné a nepodmíněné tresty za trestný čin §249b v letech 2006 - 2009

	2006	2007	2008	2009
Nepodmíněné tresty - celkem	19	25	39	25
- do 1 roku	19	23	33	22
- 1-5 let	0	2	6	3
Podmíněné tresty - celkem	213	213	213	211
- zákaz činnosti	0	0	0	0
- peněžitý trest	16	15	17	13
- obecně prospěšné práce	113	68	81	79
- trestní opatření	14	13	11	17
- jiný trest	13	11	7	10
- upuštěno od potrestání	20	15	19	22

Zdroj: Ročenky kriminality 2007 – 2010 Ministerstva spravedlnosti. Vlastní úprava

Z tabulky lze vyčíst, že za trestný čin neoprávněného držení platební karty se nejčastěji vyskytují podmíněné tresty. Mezi nepodmíněné tresty patří odnětí svobody do 1 roku. Odnětí svobody na 5-15 let, přes 15 let, či doživotí se v těchto letech za tento trestný čin vůbec nevyskytují. Mezi nejčastější podmíněné tresty patří obecně prospěšné práce.

Tabulka 3.4 zobrazuje kriminalitu za období 1.1.2010 – 31.12.2010. Jedná se o trestný čin neoprávněné držení platební karty a statistika je brána za celou Českou republiku. Z tabulky je patrné, že bylo zjištěno 8074 trestných činů neoprávněného držení platební karty, ale pouze 1703 trestných činů bylo objasněno. Rozdíl je dán tím, že u většiny trestných činů bylo ukončeno prověřování. Dále tabulka zobrazuje Počet spáchaných skutků a počet stíhaných a vyšetřovaných osob.

Celková škoda u tohoto trestného činu v tis. Kč je 339 919 Kč, z toho 16 000 Kč bylo zajištěno. [66]

[66] Internetové stránky Policie ČR. Dostupné z: <http://www.policie.cz/clanek/statisticke-prehledy-kriminality-650295.aspx>. [cit. 15. března 2011]

Tabulka 3.4 – Kriminalita za období 1.1.2010 – 31.12.2010, celá ČR

Trestný čin neoprávněné držení platební karty	Počet
Zjištěno	8074
Objasněno	1703
Spácháno skutků	1243
Stíháno, vyšetřováno osob	938

Zdroj: Statistické přehledy kriminality Policie ČR. Vlastní úprava

Tabulka 3.5 zobrazuje počet pachatelů, kteří spáchali trestný čin neoprávněného držení platební karty.

Tabulka 3.5 – Pachatelé trestného činu neoprávněné držení platební karty.

Pachatelé trestného činu	Počet
Pod vlivem	23
Alkohol	18
Recidivisté	891
Nezletilí 1-14 let	32
Mladiství 15-17 let	125

Zdroj: Statistické přehledy kriminality Policie ČR. Vlastní úprava

V tabulce 3.6 je zobrazen počet stíhaných a vyšetřovaných osob v celé České republice, které spáchali trestný čin neoprávněné držení platební karty.

Tabulka 3.6 – Počet stíhaných a vyšetřovaných osob v celé ČR

Stíhané a vyšetřované osoby	Počet
Recidivisté	536
Nezletilí 1-14 let	30
Mladiství 15-17 let	66
Ženy	306

Zdroj: Statistické přehledy kriminality Policie ČR. Vlastní úprava

V tabulce 3.7 zobrazuje kriminalitu za obodbí 1.1.2010 – 31.12.2010 trestného činu neoprávněné držení platební karty a zde jsem se zaměřila na statistiku Moravskoslezského kraje.

Celková škoda v tomto kraji byla v tis. Kč 31 523 Kč. [67]

Tabulka 3.7 – Kriminalita za období 1.1.2010 – 31.12.2010 v Moravskoslezském kraji

Trestný čin neoprávněné držení platební karty	Počet
Zjištěno	1114
Objasněno	201
Spácháno skutků	154
Stíháno, vyšetřováno osob	290

Zdroj: Statistické přehledy kriminality Policie ČR. Vlastní úprava

Tabulka 3.8 zobrazuje jednotlivé pachatelé trestného činu, kteří spáchali trestný čin neoprávněné držení platební karty v Moravskoslezském kraji.

Tabulka 3.8 – Počet pachatelů v Moravskoslezském kraji

Pachatelé trestného činu	Počet
Pod vlivem	3
Alkohol	3
Recidivisté	114
Nezletilí 1-14 let	6
Mladiství 15-17 let	11

Zdroj: Statistické přehledy kriminality Policie ČR. Vlastní úprava

Tabulka 3.9 zobrazuje počet stíhaných a vyšetřovaných osob v Moravskoslezském kraji.

[67] Internetové stránky Policie ČR. Dostupné z: <http://www.policie.cz/clanek/statisticke-prehledy-kriminality-650295.aspx>. [cit. 15. března 2011]

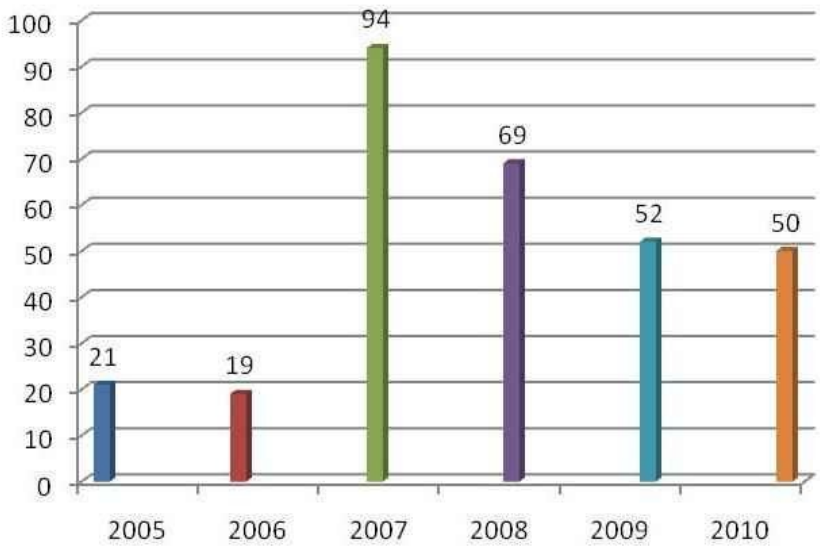
Tabulka 3.9 – Stíhané a vyšetřované osoby v Moravskoslezském kraji

Stíhané a vyšetřované osoby	Počet
Recidivisté	77
Nezletilí 1-14 let	7
Mladiství 15-17 let	11
Ženy	38

Zdroj: Statistické přehledy kriminality Policie ČR. Vlastní úprava

Následující obrázek 3.10 ukazuje počty skimmovacích zařízení včetně pokusů nasazených nástavců na bankomaty v České republice.

Obrázek 3.10 – Přehled počtu skimmování na území ČR za období 1.1.2005 do 31.12.2010



Zdroj Internetové stránky Policie ČR. Dostupné z:
<http://www.policie.cz/clanek/skimming.aspx>. [cit. 5. března 2011]

Z dostupných dat je patrné, že v roce 2005 a 2006 se pachatelé teprve učili vyrábět a používat skimmovací nástavce, často je jako polotovary nasazovali na bankomaty a na místě je dopracovávali. Většina zařízení nebyla dokonalá a bylo možné je snadno odhalit.

Rok 2007 znamenal nárůst počtu skimmovacích zařízení, lze tedy předpokládat, že pachatelé využili období let 2005 a 2006 k tomu, aby se naučili vyrábět velmi kvalitní a těžko rozpoznatelné skimmovací nástavce. Na druhou stranu se také bankovní sektor i policie z uplynulého období také poučili a přijali adekvátní opatření a to jak ve směru preventivních

opatření, tak i v informování občanů. Ze zadržených nástavců bylo zřejmé, že jsou vyráběny tzv. na koleni. Tato činnosti byla v té době doménou rumunských zločineckých gangů.

V následujícím roce 2008 se rumunské gangy stáhly a Českou republiku začali používat jako tranzitní zemí pro převozy nakradených peněz v jiných státech Evropy do Rumunska a opačně, k převozům skimmovacích zařízení. Toto dokládá pokles počtu nasazených skimmovacích zařízení. Výraznější pokles ale vyrovnaly bulharské gangy, které v tomto období začali také nasazovat skimmovací zařízení v České republice.

V letech 2009 a 2010 dochází k mírnému nárůstu počtu oproti roku 2008. Zadržená zařízení jsou velmi dobré kvality, často miniaturní a na bankomatu těžko rozpoznatelný. K jejich výrobě jsou využívány vysokoškolsky vzdělané osoby a je zřejmá vysoká organizovanost zločineckých gangů, jejich hierarchie a rozmístění po celé Evropě, včetně jejich rozšíření do Severní a Střední Ameriky včetně Asie a Austrálie.[68][

V příloze č. 9 je mapa, která znázorňuje nasazené skimmovací zařízení na bankomatech v ČR v letech 2003 – 2010 v jednotlivých městech a obcích. Z obrázku je patrné, že nejvíce skimmovacích zařízení bylo nasazeno v Praze.

Na podzim roku 1997 byl založen Bezpečnostní výbor SBK, který sdružuje pracovníky bank a dalších institucí a organizací, zabývajících se řešením podvodných transakcí. Jejich spolupráce s orgány činnými v trestním řízení v boji proti organizovaným nájezdům podvodníku nese užitek ve snižování ztrát z podvodů. Snižování znázorňuje tabula 3.11 – Podezřelé transakce – procentní body a basis points (BP). [69]

Tabulka 3.11– Podezřelé transakce – procentní body a basis points (BP)

	2001	2002	2003	2004	2005	2006	2007 (1. pol)
ČR - %	0,073	0,057	0,064	0,040	0,013	0,027	0,023
ČR - BP	7,3	5,7	6,4	4	3	2,7	2,3

Zdroj: http://www.bankovnikarty.cz/pages/czech/profil_cr.html

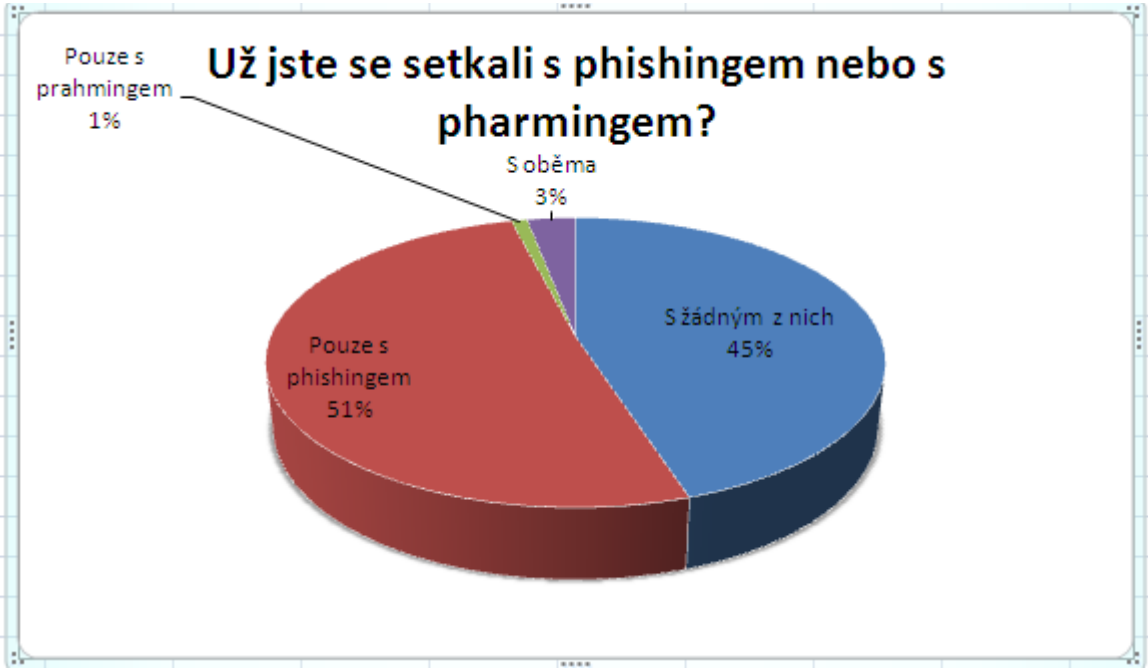
[68] Internetové stránky Karty-peníze. Dostupné z: <http://www.karty-penize.webgarden.name/menu/skimming>. [cit. 18. února 2011]

[69] Internetové stránky Bankovní karty. Dostupné z: <http://www.bankovnikarty.cz/pages/czech/profil_cr.html>.[cit. 23. února 2011]

Procentní body vyjadřují poměr celkového objemu podvodných případů, nahlášených vydavatelskými bankami, k celkovému objemu obratů uskutečněných v akceptační infrastruktuře u obchodníků a v sítí bankomatů na území ČR kartami MasterCard a Visa. [74]

Následující obrázek 3.12 zobrazuje anketu, která zkoumá, zda se někdy dotazovaní lidé setkali s phishingem či pharmingem. Odpovědělo celkem 549 respondentů. Z grafu je patrné, že více něž polovina respondentů se již setkalo s phishingem, tj. podivným emailem.

Obrázek 3.12 – Anketa



Zdroj:http://www.lupa.cz/clanky/rhybareni-strida-pharming/ Vlastní úprava

4 Prostředky k minimalizaci zneužití elektronického bankovnictví

Hlavním cílem této práce je určit prostředky k minimalizaci zneužití elektronického bankovnictví. Možnosti k omezení zneužití elektronického bankovnictví může být celá řada, jelikož existuje celá řada faktorů, které jsou pachateli trestných činů elektronického bankovnictví využívány.

Z hlediska příčin vzniku trestného činu jsem si tyto faktory rozdělila na faktory legislativní, soudní praxe, technické, kulturní a preventivní prostředky a další prostředky k minimalizaci zneužití elektronického bankovnictví.

4.1 Legislativní

Důležitá je legislativní úprava této oblasti. Jak již bylo zmíněno v této práci, konkrétně v kapitole 2.1. Právní úprava, existuje celá řada zákonů a směrnic, které se zabývají úpravou elektronického bankovnictví. Tato oblast je, jak již bylo řečeno také předmětem úpravy na úrovni EU. Dle mého názoru je tato oblast z legislativní stránky chráněna zatím dobře, i když do budoucna bude muset projít řadou novel.

4.2 Soudní praxe

V této oblasti bych doporučovala zlepšení na straně **soudů**. V kapitole 3.7 Statistika zneužití elektronického bankovnictví je zobrazena tabulka 3.2 Počet obžalovaných a odsouzených osob za trestný čin §249b v letech 2006 – 2009. Z této tabulky je patrné, že pouze část pachatelů je za tento trestný čin odsouzena. Proto bych navrhovala, aby soudy pracovaly rychleji. Tudíž by došlo k rychlejšímu vyřízení určitých kauz a trestných činů a ne jak je to doposud, kdy se jeden soudní spor vyřizuje 3 roky a déle.

4.3 Technické

Jestliže používá klient služby elektronického bankovnictví, především internetového bankovnictví, měl by používat pouze **svůj domácí počítač**, ke kterému nemají přístup cizí osoby. Jestliže by k tomuto zásahu neoprávněnou osobou mohlo dojít, je dobré používat zabezpečení počítače pomocí hesla, které ví pouze majitel počítače. K využívání služeb internetového bankovnictví bych vůbec nedoporučovala používat počítač, o kterém nic nevíme, např. počítač v internetové kavárně. Zde mohou existovat tzv. programy na odposlouchávání klávesnice, jak již bylo zmíněno v kap. 3.5 Zneužití internetového

bankovnictví, v podkapitole 3.5.1 Odposlouchávání klávesnice. Jestliže má klient přístup ke svému účtu na základě osobního certifikátu, měl by i tento certifikát chránit před zneužitím.

Také bych doporučovala používat pouze **známý bankomat**, ze kterého vybíráme často. V případě výběru u jiného bankomatu, bych doporučovala, si tento bankomat nejdříve prohlédnout, i když mnohým z nás to nijak nepomůže. Ale i přesto se může stát, že si klient všimne něčeho podezřelého.

Dále bych také doporučovala **nastavení zabezpečení internetového bankovnictví** pomocí SMS zprávy či e-mailové zprávy. Tyto zprávy informují o provedení transakce z klientova účtu, a tudíž má klient ihned přehled, jestliže došlo ke zneužití. Je to určitá kontrola pro klienta.

Asi nejdůležitějším prvkem při používání internetového bankovnictví je mít **antivirový program**, který neustále aktualizujeme. Chrání nás před škodlivými programy, jako jsou viry či spamy.

Mezi další důležité prostředky k minimalizaci zneužití elektronického bankovnictví bych uvedla **zavedení pouze čipových karet**. Čipové karty jsou mnohem bezpečnější než karty, které obsahují pouze magnetický proužek. Jestliže budu platit čipovou kartou u obchodníka, budu zadávat pouze PIN kód. Při platbě kartou s magnetickým proužkem budu zadávat PIN kód a také vlastnoruční podpis. Ale přesto je pouze ověření pomocí PIN kódu bezpečnější, jelikož tento kód zná pouze majitel platební karty, zatímco podpis jde jednoduše zneužít a napodobit, protože je zobrazen na zadní straně karty. Čipové karty jsou také hůře padělatelné a zneužívány než karty s magnetickým proužkem. Data uložená v čipu jsou chráněna, a tudíž tyto karty snižují riziko podvodných transakcí. Údaje uložené přímo v čipu jsou chráněna vysokou úrovní šifrování, tudíž nejde čip tak snadno okopírovat jako magnetický proužek, v tomto případě by se jednalo o skimming platebních karet. Čipové karty mají jak čip tak také magnetický proužek, takže pokud není obchodník zatím vybaven čipovou technologií, transakce proběhne pomocí magnetického proužku a zákazník bude vyzván k podpisu.

Dalším prostředkem k minimalizaci zneužití internetového bankovnictví bych navrhovala **technologický pokrok**. S postupem času je pro padělatele jednodušší získat prostředky k padělání platebních karet a výrobě skimmovacích zařízení sloužících ke zneužití platební karty. Důležité je také neustále zlepšovat a zdokonalovat **ochranné prvky**

platebních karet. Vymýšlet nové ochranné prvky platebních karet, které boudou pro pachatele hůře padělatelné.

4.4 Kulturní a preventivní prostředky

Mezi kulturní a preventivní prostředky k minimalizaci zneužití elektronického bankovnictví bych uvedla média, školu a rodinu.

Důležitou roli v této oblasti mají především **média**, které ovlivňují chování lidí. Mohou ukazovat jak se lidé chovat v určitých případech, či jak jednat jestliže dojde k případnému trestnému činu a na co si lidé mají případně dávat pozor a tím zlepšovat prevenci v této trestné činnosti. Ale je také pravdou, že média také ukazují jak zneužít tuto oblast a jak vypadají např. skimmovací zařízení či jiné způsoby jak zneužít elektronické bankovnictví, třeba tím, že došlo ke krádeži celého bankomatu. A i když to možná někdy neberou na vědomí nebo si to možná ani neuvědomí, tak tím dají pachatelům určitou radu, jak mohou páchat tuto trestnou činnost.

Oblasti zneužití elektronického bankovnictví se média příliš nevěnují, i když se občas v televizním či rozhlasovém vysílání doslechneme o určitém trestném činu, či dočteme v tisku. Dle mého názoru by ale měla média více informovat o této problematice, jelikož cílovou skupinou posluchačů a čtenářů jsou především školáci a mladiství a i v této věkové oblasti je již značný počet trestných činů.

Jako další prostředek, který může posloužit ke snížení kriminality v oblasti elektronického bankovnictví, bych uvedla **školu** a s tím spojené pedagogy. Pedagogové mají na starost výchovnou funkci, a tudíž by tato oblast také neměla být vynechána. Ve škole se velmi často hovoří o alkoholu, drogách, krádežím a podobných trestných činech, ale o zneužití elektronického bankovnictví se již nezmíní nikdo. Jak je patrné z kapitoly 3.7 Statistika zneužití elektronického bankovnictví, v tabulce 3.5 Pachatelé trestného činu neoprávněné držení platební karty, tak počty dětí od 1 – 14 let a mladistvých 15-17 let jsou nezanedbatelné. Tudíž bych navrhovala v rámci výuky, kdy jsou na škole prováděny určité preventivní přednášky např. v případě drog apod., zavést také přednášky týkající se zneužití elektronického bankovnictví. V dnešní době má téměř každá domácnost počítač a děti či mladiství jsou s ním denně ve styku.

Asi nejdůležitější oblastí v této skupině je **rodina**. V rodině se seznamujeme s předpokládaným chováním ve společnosti, učí nás jak reagovat na určité situace a tudíž

vytváří určitý postoj k společnosti obecně. Většinu našich návyků a způsobů si získáváme v průběhu života v rodině a také vlivem našeho okolí. Ale hlavní vliv na nás má především rodina. Jestliže rodina neplní svou funkci, má to určitě vliv na chování dítěte a tudíž ovlivnit jeho jednání v budoucnosti. Z tabulky 3.2 Pachatelé trestného činu neoprávněného držení platební karty v kapitole3.7 Statistika zneužití elektronického bankovnictví, je vidět, že tento trestný čin páchají také děti od 1-14 let. Jestliže se rodiče dostatečně nevěnují svým dětem, může to vést k nevhodnému využívání volného času a tudíž páchání trestných činů, kdy dítě ani nemusí tušit, že právě spáchal nějaký trestný čin.

4.5 Další prostředky

Dalším prostředkem proti zneužití elektronického bankovnictví, je **nepoužívat jednoduché přihlašovací heslo či PIN kód**. Jednoduché heslo jde hackery snadněji rozluštit a zneužít. Nedoporučuji používat slova a čísla, které mají nějakou souvislost se jmény v rodině, jejich datem narození, telefonním číslem apod. Banky doporučují použít kombinaci velkých a malých písmen, číslic a speciálních znaků, jako jsou tečka, vykřičník, otazník apod. Mnoho z nás si heslo zapisuje na různé papírky, do diářů, telefonu atd., což vede také k jednoduchému zneužití přísunového hesla či PIN kódu. Už vůbec nedoporučuji PIN kód nosit sebou napsaný na papírku a uložený společně s platební kartou na stejném místě. To bychom případnému zloději kartu dali jako na stříbrném podnose a než bychom zjistili, že došlo ke krádeži či ztrátě karty, mohlo by být již pozdě. V dnešní době si klient může sám zvolit PIN kód, který se mu bude dobře pamatovat, tudíž nemusí tyto velice cenné data nosit zapsané někde na papíře či v mobilu.

Na internetu bychom měli také navštěvovat pouze **známé stránky** a neměli bychom stahovat neznáme soubory, jelikož tyto soubory mohou do počítače nainstalovat také programy, pomoci nichž bude počítač ovládán na dálku nějakým hackerem a my o tom ani nemusíme tušit. Zejména se jedná o stránky s erotickým obsahem a nelegálním software. Dále nedoporučuji otevírat e-mailové zprávy od adresátů, které neznáme nebo které mají podezřelý název či obsah. Tuto zprávu doporučuji bez otevření ihned smazat.

Žádná z bank nikdy nevyžaduje sdělení PIN kódu či přístupového hesla pomocí e-mailové zprávy. V tomto případě se většinou jedná o podvodný e-mail, který bude sloužit ke zneužití. Je dobré se vždy také přesvědčit, zda se jedná opravdu o stránky banky, když se přihlašujeme do internetového bankovnictví. Toto jde ověřit tím, že vedle adresního řádku je

zobrazen žlutý zámek. Jestliže by přece jen došlo k takovémuto požadavku ze strany banky, může klient kdykoliv do banky zavolat a ověřit si to.

Jako další prostředek proti zneužití platební karty bych uvedla mít tuto kartu vždy na očích. Být velmi **obezřetný při platbě v restauraci nebo v obchodě**, např. když si číšník tuto katru vezme a po zaplacení útraty ji opět donese zpět. Číšník může vzít kartu klienta, vymluví se, že čtečku mají např. v kanceláři a tam protáhne platební kartu s magnetickým proužkem vlastní čtečkou karet a tím získá její data. Tyto data poté mohou být zaznamenány na vyrobenou falešnou platební kartu a zneužity k následnému vybírání a placení.

5 Závěr

V této diplomové práci jsem nejprve specifikovala oblast elektronického bankovnictví a popsala všechny prostředky, které tato oblast obsahuje, od platebních karet až po internetové bankovnictví a snažila se tyto prostředky popsat také z historického vývoje.

V další kapitole jsem se již zaměřila na konkrétní způsoby padělání elektronického bankovnictví, jak již zmíněných platebních karet, tak i internetového bankovnictví a dalších prostředku elektronického bankovnictví.

Na základě těchto zjištěných poznatků, jsem navrhla určité prostředky k minimalizaci zneužití elektronického bankovnictví. Jedná se o stěžejní kapitolu celé této diplomové práce a bylo to také stanoveným cílem. Tyto prostředky k minimalizaci zneužití jsem si rozdělila na legislativní, soudní praxe, technické, kulturní a preventivní prostředky a další prostředky sloužící k minimalizaci zneužití elektronického bankovnictví a v každé této oblasti navrhla určitá doporučení. V legislativní oblast je dle mého názoru zatím chráněna dobře, ale do budoucna bude muset projít řadou novel. V soudní praxi jsem navrhovala zlepšení na straně soudů. V technické oblasti jsem navrhla např. používání především svého počítače, ke kterému nemají přístup jiní lidé nebo v případě platební karty používat známý bankomat. Důležité je mít také aktualizovaný antivirový program a používat zabezpečení internetového bankovnictví, které nám pomocí SMS zprávy či e-mailové zprávy oznámí, že byla provedena určitá transakce. Důležitý je také technologický pokrok. V oblasti kulturních a preventivních prostředků jsem navrhovala především činnost médií a školu, která má výchovnou funkci a především rodinu. Poslední kapitola zahrnuje další prostředky k minimalizaci zneužití elektronického bankovnictví, kde jsem doporučovala nepoužívat jednoduché přístupové hesla a PIN kódy a už vůbec je nenosit napsané někde na papírku u karty či v mobilu. Lidé by si měli také dávat pozor při platební kartou v restauracích či obchodních řetězcích, nikdy by neměli spouštět svou platební kartu z očí.

Zajímavý pohled na problematiku zneužití elektronického bankovnictví je také ze statistického hlediska. Toto je podrobně rozebráno v kapitole 3.7 Statistika zneužívání elektronického bankovnictví.

Jak již bylo řečeno v této práci, není platebního prostředku, který by nešel zneužít, tudíž platební karty a elektronické bankovnictví nebude výjimkou. Lidé jsou stále více vynalézaví a mají stále nové nápady jak zneužívat také tuto oblast.

Tato diplomová práce mi byla přínosem, protože jsem na začátku ani netušila, kolik existuje způsobů, jak zneužít platební kartu či napadnout elektronické bankovnictví a věřím, že jsem zdaleka ještě nepopsala všechny možné způsoby zneužívání přímého bankovnictví. Již si také budu dávat pozor, především při používání internetového bankovnictví. Každý den o tom slýcháme v televizi a čteme v novinách, ale každý z nás si řekne: „mě se to netýká“, jenže je velmi jednoduché přijít o peníze a ani o tom nemusíme tušit.

Seznam použité literatury

Monografie

[1] ČASTORÁL, Z. *Ekonomická kriminalita*. 1. vydání. Praha: Eupress, 2007. 184 s. ISBN 978-80-86754-83-3

[2] DVOŘÁK, P. *Bankovnictví pro bankéře a klienty*. 3. vydání. Praha: Linde. 2005. 681s. ISBN 80-7201-515-X

[3] GŘIVNA, T.; POLČÁK R. *Kyberkriminalita a právo*. 1 vydání. Praha: Auditorium. 2008. 220s. ISBN 978-80-903786-7-4

[4] JIROVSKÝ, V. *Kybernetická kriminalita*. 1. vydání. Praha: Grada Publishing. 2007. 288s. ISBN 978-80-247-1561-2

[5] JUŘÍK, P. *Platební karty – velká encyklopedie 1870 - 2006*. 1 vydání. Praha: Grada Publishing, 2006. 296s. ISBN 80-247-1381-0

[6] JUŘÍK, P. *Svět platebních a identifikačních karet*. 2. vydání. Praha: Grada Publishing, 2001. 184s. ISBN 80-247-0195-2

[7] LANCE, J. *Phishing bez záhad*. 1. vydání. Praha: Grada Publishing. 2007. 284s. ISBN 978-80-247-1766-1

[8] MÁČE, M. *Platební styk – klasický a elektronický*. 1 vydání. Praha: Grada Publishing, 2006. 220s. ISBN 80-247-1725-5.

[9] PŘÁDKA, M.; KALA, J. *Elektronické bankovnictví*. 1 vydání. Praha: Computer Press, 2000. 166s. ISBN 80-7226-328-5.

Právní předpisy

[10] Zákon č. 284/2009 Sb., o platebním styku, ve znění pozdějších předpisů.

[11] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

Elektronické zdroje

[12] SADOVSKÝ, Dalibor; SUCHÁNEK, Jaroslav. Platební karty a možnosti jejich zneužití. Kriminalistika [online]. 2004, č. 1 [cit. 9. února 2011]. Dostupné z: <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2004/0401/suchanek_info.html>

[13] Internetové stránky Sdružení pro bankovní karty. Dostupné z: <http://www.bankovnikarty.cz/pages/czech/profil_cr.html>.[cit. 23. února 2011]

[14] Internetové stránky BusinessCenter. Zákon o platebním styku. Dostupné z: <http://business.center.cz/business/pravo/zakony/platebni_styk/>.[cit. 25. února 2011]

[15] Internetové stránky CEED. Elektronické bankovnictví. Dostupné z: <http://www.ceed.cz/bankovnictvi/778elektronicke_bankovnictvi.htm>.[cit. 23. února 2011]

[16] Internetové stránky České spořitelny. Znáte základní finty počítačové kriminality? Neskočte na ně! Dostupné z: <http://www.csas.cz/banka/content/inet/internet/cs/letak_hoax.pdf>. [cit. 7. dubna 2011]

[17] Internetové stránky České spořitelny. Internetbanking České spořitelny. Dostupné z: < https://www.servis24.cz/ebanking-s24/dispatcher>. [cit. 15. února 2011]

[18] Internetové stránky Eur-lex.europa.eu. Směrnice Evropského parlamentu a Rady 97/7/ES ze dne 20. května 1997 o ochraně spotřebitele v případě smluv uzavíraných na dálku. Dostupné z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0007:CS:HTML/>. [cit. 14. února 2011]

[19] Internetové stránky Eur-lex.europa.eu. Směrnice Evropského parlamentu a Rady 200/46/ES ze dne 18. září 2000 o přístupu k činnosti institucí elektronických peněz , o jejím výkonu a o obezřetnostem dohledu nad touto činností. Dostupné z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0046:CS:HTML>.[cit. 14. února 2011]

[20] Internetové stránky Eur-lex.europa.eu. Směrnice Evropského parlamentu a Rady 2002/65/ES ze dne 23. září 2002 o uvádění finančních služeb pro spotřebitele na trh na dálku a o změněn směrnice Rady 90/619/EHS a směrnice 98/27/ES. Dostupné z: <http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0065:CS:HTML>.[cit. 14. února 2011]

[21] Internetové stránky FinExpert. O bezpečnosti přímého bankovnictví s prof. Smejkalem. Dostupné z <http://finexpert.e15.cz/o-bezpecnosti-primeho-bankovnictvi-s-prof-smejkalem>. [cit. 7. dubna 2011]

[22] Internetové stránky Hoax. Co je to phishing. Dostupné z: <http://www.hoax.cz/phishing/co-je-to-phishing>. [cit. 18. února 2011]

[23] Internetové stránky Karty-peníze. Skimming. Dostupné z: <http://www.karty-penize.webgarden.name/menu/skimming>. [cit. 18. února 2011]

[24] Internetové stránky Konzument. Evropská dokumentace o potírání podvodů při bezhotovostních platbách. Dostupné z: <http://www.konzument.cz/publikace/soubory/pruvodce_spotrebitele/EvropDokumentace_podvody.pdf>.[cit. 23. února 2011]

[25] Internetové stránky Lupa.cz. Rhybaření střídá pharming. Dostupné z: <http://www.lupa.cz/clanky/rhybareni-strida-pharming/>.[cit. 24. února 2011]

[26] Internetové stránky Lupa.cz. Většina českých bank není odolný proti clicjack. Dostupné z: <http://www.lupa.cz/zpravicky/vetsina-ceskych-bank-neni-odolna-proti-clickjack>.[cit. 20. února 2011]

[27] Internetové stránky Měšec. Jak je zabezpečené internetové bankovnictví. Dostupné z: <http://www.mesec.cz/clanky/jak-je-zabezpecene-internetove-bankovnictvi//>.[cit. 24. února 2011]

[28] Internetové stránky Peníze.cz. Internetové bankovnictví: jsou vaše peníze v bezpečí? Dostupné z: <http://www.penize.cz/bezne-ucty/18366-internetove-bankovnictvi-jsou-vase-penize-v-bezpeci>. [cit. 11. února 2011]

[29] Internetové stránky Peníze. cz. Čekdok, Tuzek a český karetní boom. Dostupné z: <http://www.penize.cz/platebni-karty/16363-cedok-tuzex-a-cesky-karetni-boom>.[cit. 4. ledna 2011]

[30] Internetové stránky Peníze.cz. Odkud kam míří český internetbanking. Dostupné z: <http://www.penize.cz/prime-bankovnictvi/42614-odkud-kam-miri-cesky-internetbanking>. [cit. 4. ledna 2011]

[31] Internetové stránky Php.vrana.cz. Cross site regest foyery. Dostupné z: <http://php.vrana.cz/cross-site-request-forgery.php>.[cit. 21. února 2011]

[32] Internetové stránky Platební–karty.info. Platební karty. Dostupné z

<http://platebni-karty.info/index.php>. [cit. 4. února 2011]

[33] Internetové stránky Pohoda. Homebanking. Dostupné z: <http://www.pohoda-prodej-instalace-sprava.cz/produkty/funkcni-moduly/homebanking-pohoda/>. [cit. 23 března 2011]

[34] Internetové stránky Policie ČR. Statistické přehledy kriminality. Dostupné z: <http://www.policie.cz/clanek/statisticke-prehledy-kriminality-650295.aspx//>.[cit. 15. března 2011]

[35] Internetové stránky Sdružení českých spotřebitelů. Podvody v e-bankovnictví. Dostupné z: <http://www.prevencepodvodu.cz/platebni-prostredky/bezhotovostni-platby/bankomat-atm.php>. [cit. 9. února 2011]

[36] Internetové stránky Trojanhelp. Pharming. Dostupné z: <http://trojanhelp.wz.cz/pharming.htm>. [cit. 7. dubna 2011]

[37] Internetové stránky Wikipedia. Clikjacking. Dostupné z: <http://cs.wikipedia.org/wiki/Clickjacking>.[cit. 21. února 2011]

[38] Internetové stránky Wikipedia Cross site regest foyery. Dostupné z: <http://cs.wikipedia.org/wiki/Cross-site_request_forgery>.[cit. 21. února 2011]

[39] Internetové stránky Wikipedia. Cross site scripting. Dostupné z: <http://cs.wikipedia.org/wiki/Cross-site_scripting>.[cit. 21. února 2011]

[40] Internetové stránky Wikipedia. Platební karta. Dostupné z: <http://cs.wikipedia.org/wiki/Platebn%C3%AD_karta>.[cit. 3. ledna 2011]

[41] Internetové stránky Zlatá koruna. Co byste měli vědět o elektronickém bankovnictví. Dostupné z: <http://www.zlatakoruna.info/clanky/21-2-elektronicke-bankovnictvi/14561-co-byste-meli-vedet-o-elektronickem-bankovnictvi>. [cit. 7. února 2011]

Seznam zkratek

BP	basis point
ČSOB	Československá obchodní banka
ČR	Česká republika
ČS	Česká spořitelna
ČSSR	Československá socialistická republika
EU	Evropská unie
ISO	International Organization for Standardization
KB	Komerční banka
PIN	personal identification number
RVHP	Rada vzájemné hospodářské pomoci
SBČS	Státní banka československá
SIM	subscriber identity module
SMS	Short message service
USA	United States of America
USB	Universal Serial Bus
WAP	Wireless Application Protocol
WWW	World Wide Web

Prohlášení o využití výsledků bakalářské práce

Prohlašuji, že

- jsem byla seznámena s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická Univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečné, ke své vnitřní potřebě, diplomovou práci užít (§ 35 odst. 3)
- souhlasím s tím, že jeden výtisk bude uložen u vedoucího diplomové práce. Souhlasím s tím, že bibliografické údaje o diplomové práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou práci, nebo poskytnou licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 29. 4. 2011

Bc. Lucie Stušová

Adresa trvalého pobytu:

K Bezdínku 84
735 53 Dolní Lutyně

Přílohy

Příloha č. 1 – Skimmovací nástavce na bankomatech

Příloha č. 2 – Upravené pokladní terminály

Příloha č. 3 – Skimmovací zařízení čerpacích stanic

Příloha č. 4 – Lisabonská smyčka

Příloha č. 5 – Hradecká lišta

Příloha č. 6 – První phishingový útok v České republice na klienty CityBank

Příloha č. 7 – První phishingový útok na klienty České spořitelny

Příloha č. 8 – Další phishingový útok na klienty České spořitelny

Příloha č. 9 – Skimmovací zařízení na bankomatech v ČR v letech 2003 – 2010 v jednotlivých městech a obcích

Příloha č. 1 – Skimmovací nástavce na bankomatu

Obr. 1 – Bankomat bez skimmovacích nástavců

Zdroj: Internetové stránky Karty-peníze. Dostupné z: <http://www.karty-penize.webgarden.name/menu/skimming>. [cit. 18. února 2011]

Obr. 2 – Bankomat se skimmovacími nástavci

Zdroj: Internetové stránky Karty-peníze. Dostupné z: <http://www.karty-penize.webgarden.name/menu/skimming>. [cit. 18. února 2011]

Obr. 3 – Bankomat bez skimmovacích nástavců

Zdroj: Internetové stránky Karty-peníze. Dostupné z: <http://www.karty-penize.webgarden.name/menu/skimming>. [cit. 18. února 2011]

Obr. 4 – Bankomat se skimmovacími nástavci

Zdroj: Internetové stránky Karty-peníze. Dostupné z: <http://www.karty-penize.webgarden.name/menu/skimming>. [cit. 18. února 2011]Příloha č. 3 – Upravené pokladní terminály

Příloha č. 2 – Skimmovací nástavce na bankomatu

Obr. 1 – Upravený pokladní terminál

Zdroj: Internetové stránky Karty-peníze. Dostupné z: <http://www.karty-penize.webgarden.name/menu/skimming>. [cit. 18. února 2011]

Obr. 2 – Upravený pokladní terminál

Zdroj: Internetové stránky Karty-peníze. Dostupné z: <http://www.karty-penize.webgarden.name/menu/skimming>. [cit. 18. února 2011]

Příloha č. 3 – Skimmovací zařízení čerpacích stanic

Obr. 1 – Skimmovací zařízení na stojanu na čerpací stanici

Zdroj Internetové stránky Karty-peníze. Dostupné z: <http://www.karty-penize.webgarden.name/menu/skimming>. [cit. 18. února 2011]

Obr. 2 – Detail skimmovacího zařízení na stojanu čerpací stanice

Zdroj: Internetové stránky Karty-peníze. Dostupné z: <http://www.karty-penize.webgarden.name/menu/skimming>. [cit. 18. února 2011]

Příloha č. 4 – Lisabonská smyčka

Obr. 1 – Lisabonská smyčka

Zdroj: Internetové stránky Karty-peníze. Dostupné z: < http://www.karty-penize.webgarden.name/menu/atm-jine-utoky>. [cit. 18. února 2011]

Obr. 2 – Lisabonská smyčka

Zdroj: Internetové stránky Karty-peníze. Dostupné z: < http://www.karty-penize.webgarden.name/menu/atm-jine-utoky>. [cit. 18. února 2011]

Obr. 3 – Lisabonská smyčka

Zdroj: Internetové stránky Karty-peníze. Dostupné z: < http://www.karty-penize.webgarden.name/menu/atm-jine-utoky>. [cit. 18. února 2011]

Příloha č. 5 – Hradecká lišta

Obr. 1 – Hradecká lišta

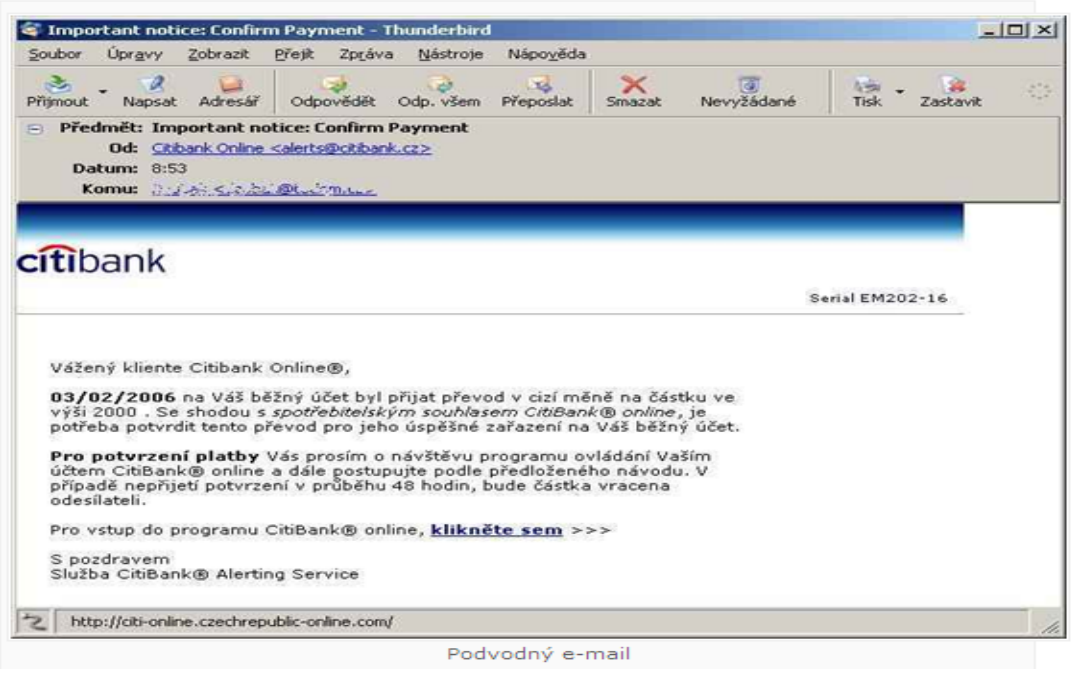
Zdroj: Internetové stránky Karty-peníze. Dostupné z: < http://www.karty-penize.webgarden.name/menu/atm-jine-utoky>. [cit. 18. února 2011]

Obr. 2 – Hradecká lišta

Zdroj: Internetové stránky Karty-peníze. Dostupné z: < http://www.karty-penize.webgarden.name/menu/atm-jine-utoky>. [cit. 18. února 2011]

Příloha č. 6 – První phishingový útok v České republice na klienty CitiBank

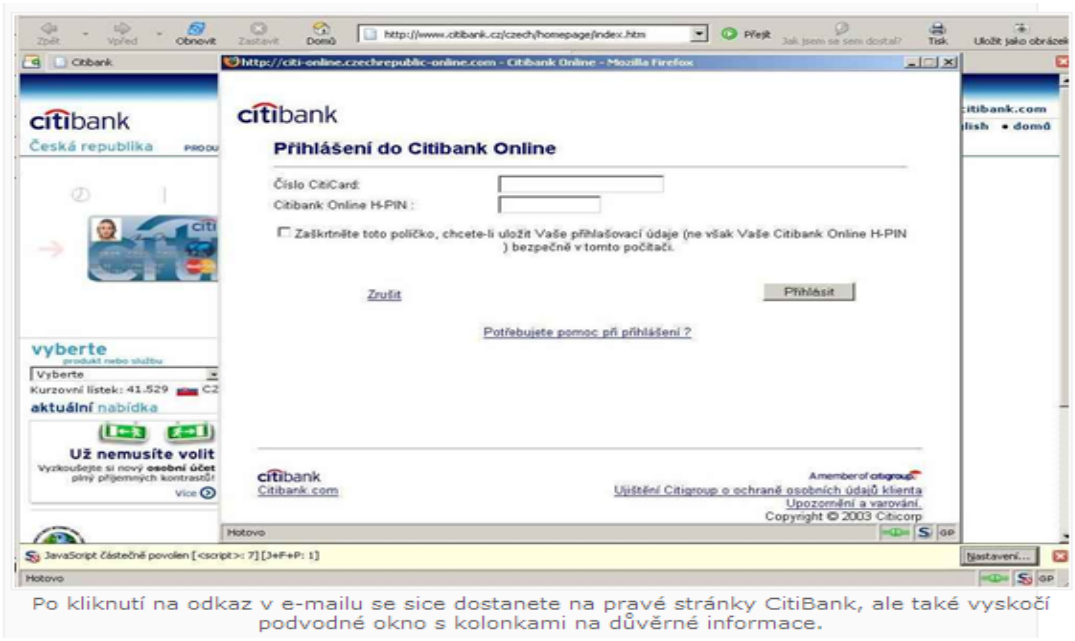
Obr. 1 – Podvodný e-mail



Podvodný e-mail

Zdroj: Internetové stránky Hoax. Dostupné z: <http://www.hoax.cz/phishing/index.php?action=hoax_detail&id=522>. [cit. 18. února 2011]

Obr. 2 – Podvodné okno

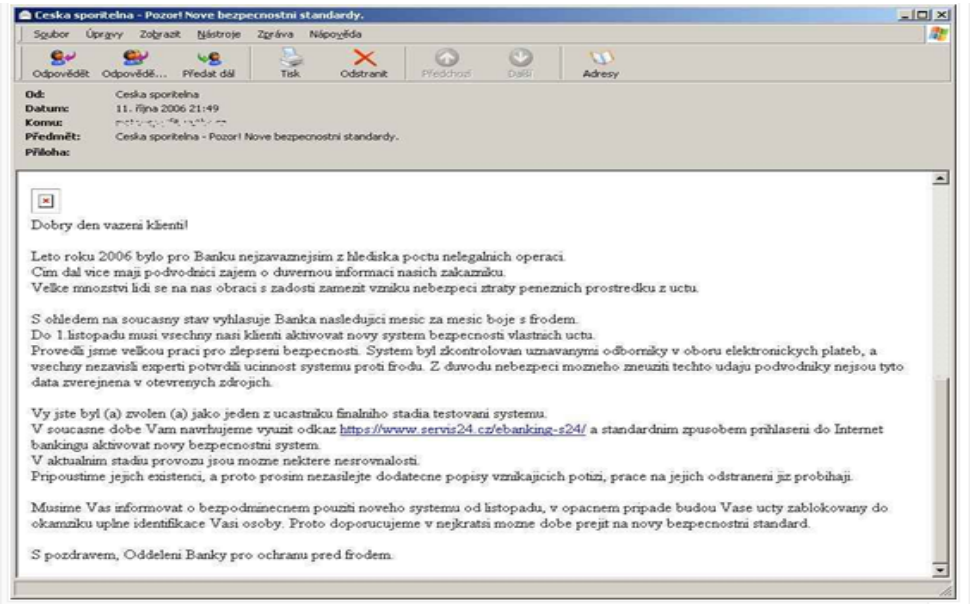


Po kliknutí na odkaz v e-mailu se sice dostanete na pravé stránky CitiBank, ale také vyskočí podvodné okno s kolonkami na důvěrné informace.

Zdroj: Internetové stránky Hoax. Dostupné z: <http://www.hoax.cz/phishing/index.php?action=hoax_detail&id=522>. [cit. 18. února 2011]

Příloha č. 7 – První phisingový útok na klienty České spořitelny

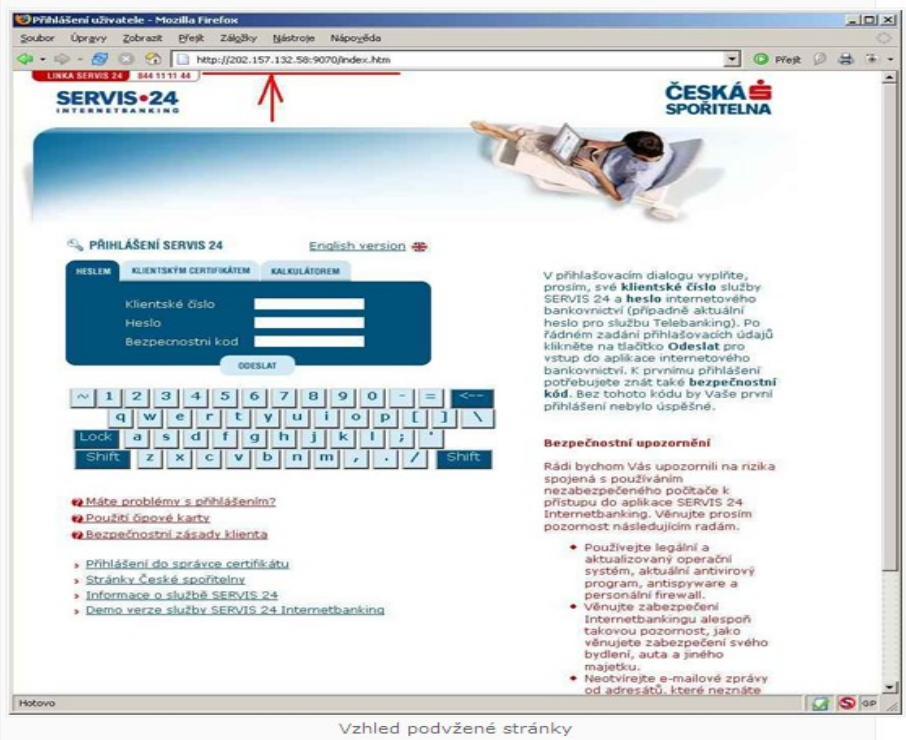
Obr. 1 – Podvodný e-mail



Vzhled podvrženého e-mailu (vzdálený obrázek se nepodařilo načíst)

Zdroj: : Internetové stránky Hoax. Dostupné z:
<http://www.hoax.cz/phishing/index.php?action=hoax_detail&id=590>. [cit. 18. února 2011]

Obr. 2 – Vzhled podvržené stránky

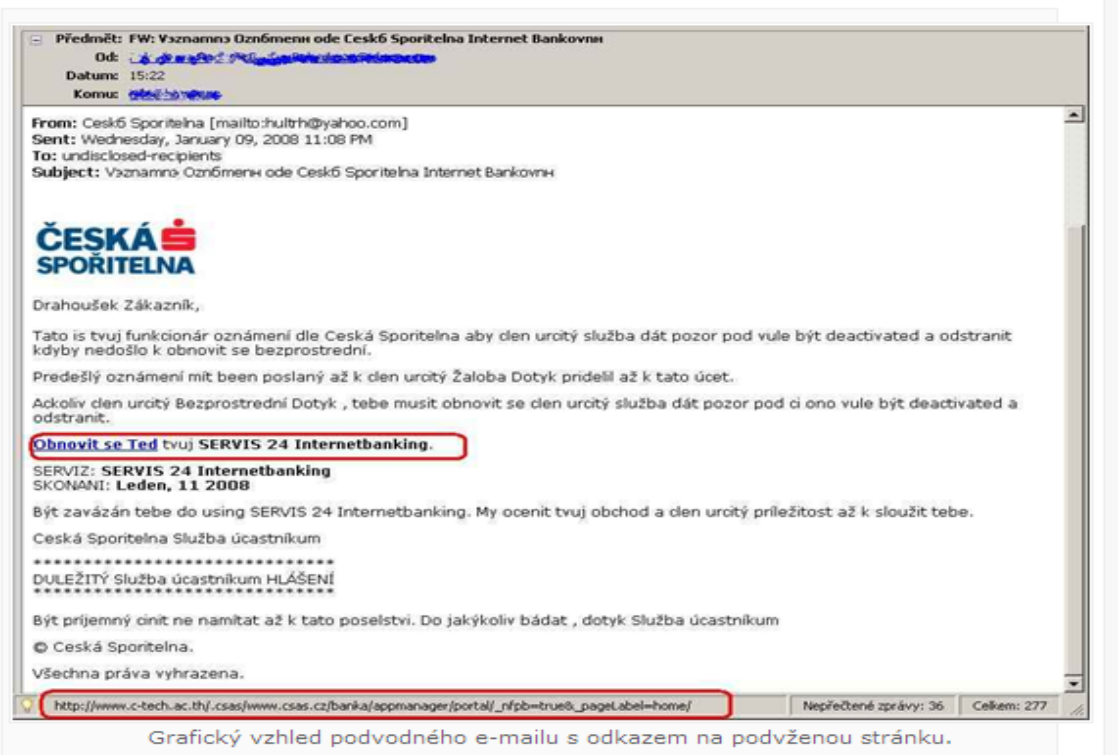


Vzhled podvržené stránky

Zdroj: : Internetové stránky Hoax. Dostupné z:
< http://www.hoax.cz/phishing/index.php?action=hoax_detail&id=590>. [cit. 18. února 2011]

Příloha č.8 – Další phishingové útoky na klienty České spořitelny

Obr.1 - Drahoušek zákazník

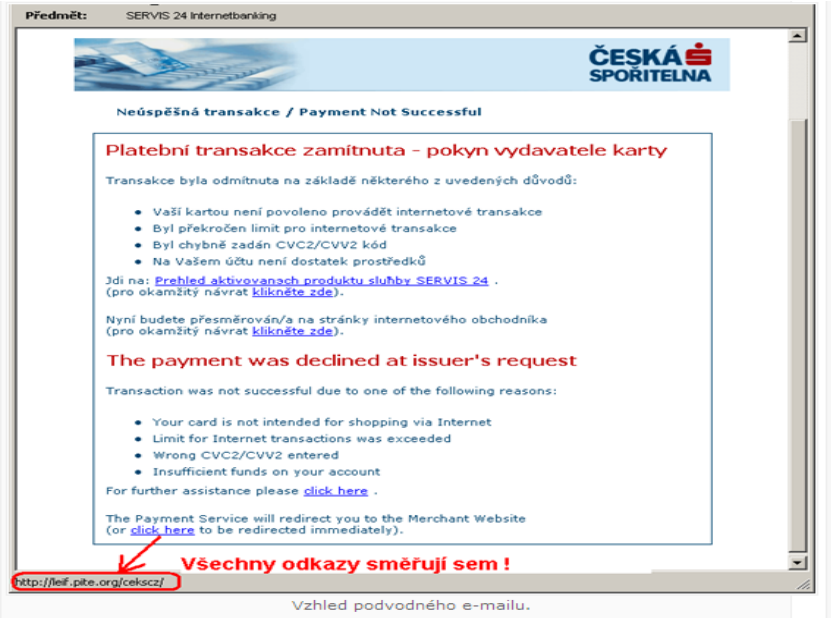


Grafický vzhled podvodného e-mailu s odkazem na podvženou stránku.

Zdroj: : Internetové stránky Hoax. Dostupné z:

< http://www.hoax.cz/phishing/index.php?action=hoax_detail&id=743>. [cit. 18. února 2011]

Obr.2 – Podvodný e-mail upozorňující na neprovedenou transakci

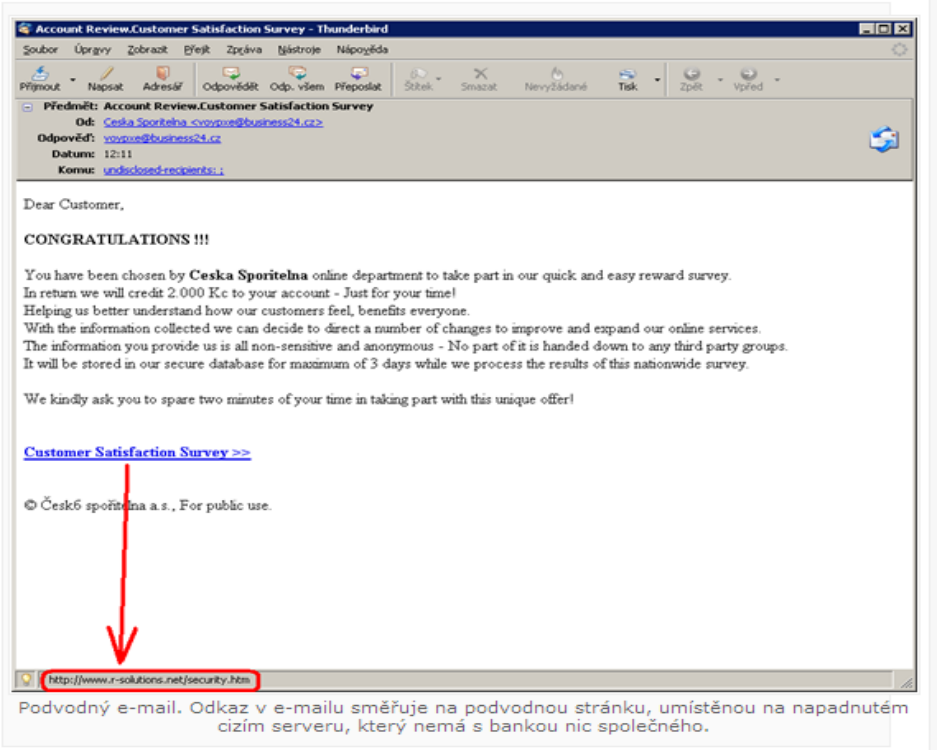


Vzhled podvodného e-mailu.

Zdroj: : Internetové stránky Hoax. Dostupné z:

< http://www.hoax.cz/phishing/index.php?action=hoax_detail&id=772>. [cit. 18. února 2011]

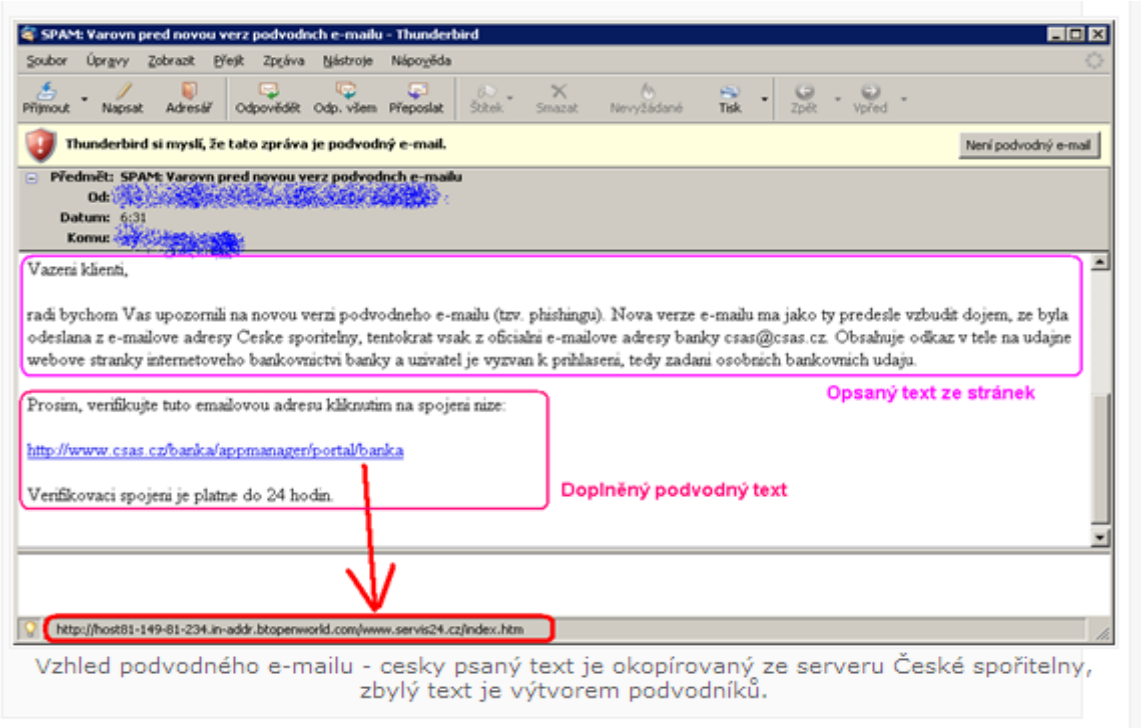
Obr.3 – Podvodný e-mail slibující odměnu za vyplnění dotazníku



Podvodný e-mail. Odkaz v e-mailu směřuje na podvodnou stránku, umístěnou na napadnutém cizím serveru, který nemá s bankou nic společného.

Zdroj: : Internetové stránky Hoax. Dostupné z:
< http://www.hoax.cz/phishing/index.php?action=hoax_detail&id=785>. [cit. 18. února 2011]

Obr. 4 – Podvodný e-mail upozorňující na sám sebe

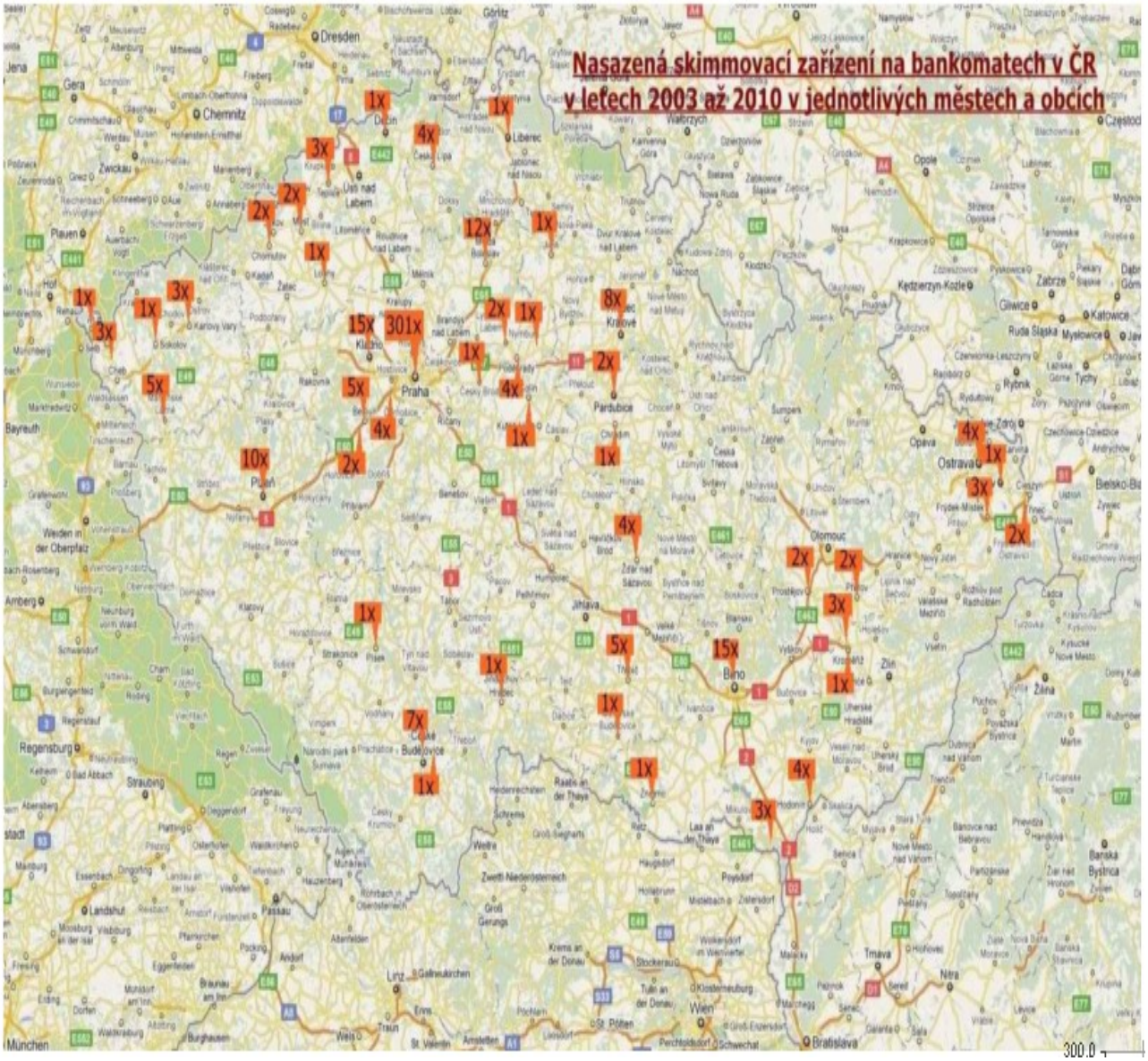


Vzhled podvodného e-mailu - cesky psaný text je okopírovaný ze serveru České spořitelny, zbylý text je výtvorem podvodníků.

Zdroj: : Internetové stránky Hoax. Dostupné z:
<http://www.hoax.cz/phishing/index.php?action=hoax_detail&id=798>. [cit. 18. února 2011]

Příloha č. 9 – Skimmovací zařízení na bankomatech v ČR v letech 2003 – 2010 v jednotlivých městech a obcích

Obrázek 1 – Mapa zobrazující nasazená skimmovací zařízení v ČR



Zdroj: Internetové stránky Karty-peníze. Dostupné z: < http://www.karty-penize.webgarden.name/thema/skimming-v-cr>. [cit. 18. února 2011]